ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72498— 2025

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ИНТЕРОПЕРАБЕЛЬНОСТИ

Определение существенных угроз и условий

Издание официальное

Москва
Российский институт стандартизации
2026

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Институт стандартизации информационных технологий» (ООО «ИСИТ»), Комиссией Российской академии наук по техногенной безопасности и Научным советом Российской академии наук «Информационная безопасность»

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 декабря 2025 г. № 1873-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

Введение

Настоящий стандарт расширяет комплекс национальных стандартов системной инженерии. В общем случае для систем различного функционального назначения актуальные задачи системной инженерии связаны:

- с реализацией государственной стратегии в экономике;
- обеспечением безопасности и устойчивого развития регионов;
- обеспечением качества функционирования и развитием народнохозяйственных, инженерно-технических, энергетических, транспортных систем, систем связи и коммуникаций;
- обеспечением безопасности систем жизнеобеспечения и жизнедеятельности человека;
- обеспечением эффективности оборонно-промышленного комплекса;
- развитием критических технологий (например, компьютерного моделирования; информационных и когнитивных технологий; технологий информационных, управляющих, навигационных систем; технологий поиска, разведки, разработки месторождений полезных ископаемых и их добычи; технологий атомной энергетики; технологий предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера);
- обеспечением безопасности критической информационной инфраструктуры, информационной и информационно-психологической безопасности;
- обеспечением промышленной безопасности, технической диагностики, управления ресурсом эксплуатации критически важных объектов и систем;
- обеспечением энергетической безопасности (в том числе функционирования и развития топливно-энергетического комплекса, нефтяной, газовой и нефтехимической промышленности, электроэнергетики, трубопроводного транспорта);
- обеспечением ядерной и радиационной безопасности;
- обеспечением безопасности горнодобывающей промышленности;
- обеспечением продовольственной безопасности;
- обеспечением экологической безопасности, экодиагностики и охраны природы;
- обеспечением безопасности освоения континентальных шельфов;
- решением иных задач обеспечения национальной безопасности и всестороннего развития Российской Федерации (см. [1] — [12]).

При решении задач системной инженерии к различным системам предъявляют требования обеспечения интероперабельности, под которой понимают способность двух или более систем или компонентов к обмену необходимой информацией и к использованию информации, полученной в результате такого обмена, т. е. требования интероперабельности свойственны практически для всех систем, независимо от их масштабов и функционального назначения.

Для рационального выполнения требований интероперабельности в жизненном цикле (ЖЦ) систем наряду с другими требованиями используют системный анализ. Как научный метод системного познания системный анализ интероперабельности предназначен для решения практических задач системной инженерии путем представления рассматриваемых системных процессов или систем в виде приемлемых моделируемых систем, обладающих свойствами интероперабельности.

Цель разработки настоящего стандарта состоит в обеспечении системного анализа интероперабельности различных систем для определения существенных угроз и условий при решении практических задач системной инженерии.

Настоящий стандарт предназначен для использования как самостоятельно, так и во взаимосвязи с другими национальными стандартами в области системной инженерии. Настоящий стандарт рекомендован к применению организациями, участвующими в создании (модернизации, развитии) и эксплуатации различных систем в части системного анализа качества, безопасности, эффективности и управления рисками.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ИНТЕРОПЕРАБЕЛЬНОСТИ

Определение существенных угроз и условий

Systems engineering. System analysis of interoperability.
Identification of significant threats and conditions

Дата введения — 2026—02—01

1 Область применения

Областью применения настоящего стандарта являются системы различного функционального назначения в их ЖЦ. Настоящий стандарт описывает общие положения и рекомендации по определению существенных угроз и условий методами системного анализа.

В приложениях А и Б приведены примеры формализации для прогнозирования рисков, примеры возможных угроз и условий нарушения интероперабельности. В приложении В приведены ссылки на стандарты системной инженерии, указывающие типовые модели, методы и методики для определения существенных угроз и условий при реализации стандартизованных процессов ЖЦ различных систем.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ГОСТ Р 27.102 Надежность в технике. Надежность объекта. Термины и определения

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

ГОСТ Р 55062 Информационные технологии. Интероперабельность. Основные положения

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

ГОСТ Р 58606/ISO/IEC/IEEE 15939:2017 Системная и программная инженерия. Процесс измерения

Издание официальное

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 59797 Информационные технологии. Сложные системы. Интероперабельность. Основные положения

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

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

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

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

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

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

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

ГОСТ Р 70569 Информационные технологии. Сетецентрические информационно-управляющие системы. Интероперабельность

ГОСТ Р 71303 Системная и программная инженерия. Возможности программных инструментариев для организационного управления инцидентами. Общие положения

ГОСТ Р 71438 Информационные технологии. Оценка процессов. Система измерения процессов для оценки их возможностей

ГОСТ Р 71440 Информационные технологии. Оценка процессов. Руководство по определению рисков в процессах

ГОСТ Р 71998 Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

ГОСТ Р ИСО/МЭК 20000-1 Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов

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 33001 Информационные технологии. Оценка процесса. Понятия и терминология

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

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

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

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 и определения

В настоящем стандарте применены термины по ГОСТ Р 27.101, ГОСТ Р 27.102, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 33001, ГОСТ Р 58606, ГОСТ Р 59853, ГОСТ Р 59989,

ГОСТ Р 59994, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1

актуальность информации: Свойство безошибочной информации (в том числе подлежащей последующей функциональной обработке или полученной в результате обработки) отражать текущее состояние прикладной области системы со степенью приближения, достаточной для получения на ее основе достоверной выходной информации в интересах конечного пользователя. Актуальность характеризует старение информации во времени.

[ГОСТ Р 59341—2021, пункт 3.1.2]

3.2

безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

[ГОСТ Р 50922—2006, статья 2.4.5]

3.3

безошибочность информации: Свойство информации не иметь явных или скрытых ошибок и/или искажений.

[ГОСТ Р 59341—2021, пункт 3.1.4]

3.4

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.5

достоверность информации: Свойство информации отражать реальное или оцениваемое состояние объектов и процессов прикладной области со степенью приближения, обеспечивающей эффективное использование этой информации согласно целевому назначению системы. Достоверность выходной информации определяется истинностью исходных данных, безошибочностью входной информации, корректностью обработки, безошибочностью при хранении и передаче информации и сохранением ее актуальности на момент использования.

[ГОСТ Р 59341—2021, пункт 3.1.6]

3.6

защита информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

[ГОСТ Р 50922—2006, статья 2.1.1]

3.7

защита информации от непреднамеренного воздействия: Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

[ГОСТ Р 50922—2006, статья 2.3.4]

3.8

защита информации от несанкционированного воздействия; ЗИ от НСВ: Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

[ГОСТ Р 50922—2006, статья 2.3.3]

3.9

защита информации от несанкционированного доступа; ЗИ от НСД: Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание — Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

[ГОСТ Р 50922—2006, статья 2.3.6]

3.10

защита информации от утечки: Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание — Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

[ГОСТ Р 50922—2006, статья 2.3.2]

3.11 **интегральный риск нарушения интероперабельности системы с учетом дополнительных специфических требований:** Сочетание вероятности того, что будут нарушены требования к интероперабельности системы либо дополнительные специфические требования (например, по защите информации), либо и то, и другое с тяжестью возможного ущерба.

3.12

интероперабельность: Способность двух или более систем или компонентов к обмену необходимой информацией и к использованию информации, полученной в результате обмена.

[Адаптировано из ГОСТ Р 55062—2021, пункт 3.1.8]

3.13

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

[ГОСТ Р 59341—2021, пункт 3.1.13]

3.14

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

[Адаптировано из ГОСТ Р 59341—2021, пункт 3.1.14]

3.15

контекст использования (для моделируемой системы): Пользователи, задачи, оборудование (аппаратные средства, программные средства, материалы), физическая и социальная среда и условия, в которых используется моделируемая система, сценарии возникновения и развития угроз нормальному использованию, реализуемые способы и технологии противодействия угрозам интероперабельности и восстановления необходимой целостности моделируемой системы после реализации угроз.

[Адаптировано из ГОСТ Р ИСО/МЭК 25000—2021, пункт 4.2]

3.16

корректность обработки информации в системе: Свойство системы обеспечивать получение правильных согласованных результатов или эффектов обработки информации.

[ГОСТ Р 59341—2021, пункт 3.1.15]

3.17 **модель системы (подсистемы, компонента, элемента системы):** Результат преобразования реальной системы (подсистемы, компонента, элемента системы) по определенной логике к формализованному представлению с направленностью на подчеркивание тех свойств, которые важны для исследования критичных сущностей этой системы (подсистемы, компонента, элемента системы) при использовании по назначению.

Примечание — См. также определение моделируемой системы в ГОСТ Р 59994—2022, пункт 3.1.4.

3.18

надежность предоставления информации в системе: Свойство системы обеспечивать прием, автоматическую обработку запроса или команды и предоставление или принудительную выдачу выходной информации согласно функциональному алгоритму при соблюдении эксплуатационных условий применения и технического обслуживания системы.

[ГОСТ Р 59341—2021, пункт 3.1.17]

3.19

полнота выходной информации в системе: Свойство выходной информации отражать состояния всех требуемых объектов учета предметной области системы. Слагается из полноты реализации функций системы, полноты ввода первоначальной информации и полноты оперативного отражения объектов учета в системе.

[ГОСТ Р 59341—2021, пункт 3.1.22]

3.20

полнота оперативного отражения объектов учета в системе: Свойство системы отражать требуемые состояния реально существующих объектов учета, в том числе впервые появляющихся в процессе функционирования системы и подлежащих учету в системе согласно ее функциональному назначению.

[ГОСТ Р 59341—2021, пункт 3.1.23]

3.21

принятие решения в режиме реального времени: Принятие решения по реализации предупреждающих действий или возможного решения об осознанном бездействии в сложившихся условиях за такое время, в течение которого выполнение этих предупреждающих действий является практически осуществимым и обоснованно целесообразным.

[ГОСТ Р 59341—2021, пункт 3.1.24]

3.22

работоспособное состояние: Состояние элемента, характеризуемое его способностью выполнять требуемую функцию, предполагая, что внешними ресурсами, при необходимости, элемент обеспечен.

[ГОСТ Р 57329—2016, статья 6.5]

3.23

риск: Следствие влияния неопределенности на достижение поставленных целей.

Примечание 1 — Под следствием влияния неопределенности понимается отклонение от ожидаемого результата. Оно может быть положительным, отрицательным или тем и другим и может рассматривать, подготавливать или приводить к возникновению возможностей и угроз.

Примечание 2 — Цели могут иметь различные аспекты и категории и распространяться на различные уровни.

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

[ГОСТ Р ИСО 31073—2024, статья 3.1.1]

3.24

своевременность предоставления требуемой информации в системе: Свойство системы обеспечивать предоставление запрашиваемой или выдаваемой принудительно (автоматически) выходной информации в задаваемые сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы.

[ГОСТ Р 59341—2021, пункт 3.1.26]

3.25

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

Примечания

1 Система — широкое понятие, может рассматриваться, например, как какой-то продукт или предоставляемые услуги, как комплекс мер по управлению или по обеспечению безопасности и работоспособности какого-либо объекта, как экономический регион, как репутация политического деятеля или совокупность мер по защите духовно-нравственных ценностей в обществе.

2 На практике интерпретация данного термина зачастую уточняется с помощью ассоциативного существительного, например система самолета.

[ГОСТ Р 57193—2025, пункт 3.1.39]

3.26

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

[ГОСТ Р 59343—2021, пункт 3.1.14]

3.27

системный анализ интероперабельности: Научный метод системного познания, предназначенный для решения практических задач системной инженерии путем представления рассматриваемых системных процессов или системы в виде приемлемой моделируемой системы, обладающей способностью к обмену необходимой информацией с другой моделируемой системой.

Примечания

1 Метод включает:

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

- обоснование с использованием моделирования предложений по обеспечению и повышению качества, безопасности и/или эффективности рассматриваемой системы (и/или ее элементов) и достижению целей системной инженерии при задаваемых ограничениях в задаваемый период времени.

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

[Адаптировано из ГОСТ Р 59991—2022, пункт 2.5]

3.28

системный элемент: Представитель совокупности элементов, образующих систему.

Пример — Системный элемент может представлять собой технические и программные средства, данные, людей, процессы (например, процессы для обеспечения услуг пользователям), процедуры (например, инструкции оператору), средства, материалы и природные объекты (например, вода, живые организмы, минералы) или любые их сочетания.

Примечание — Системный элемент является отдельной частью системы, которая может быть создана для полного выполнения заданных требований.

[ГОСТ Р 57193—2025, пункт 3.1.41]

3.29

сопровождение системы: Комплекс технических, технологических операций и организационных действий, направленных на поддержку работоспособности, устранение неисправностей, обеспечение и/или повышение безопасности, качества и эффективности системы при ее эксплуатации.

Примечание — Сопровождение системы включает в себя техническое обслуживание и ремонт отдельного технического оборудования и комплексов оборудования, сопровождение программных средств и систем, поддержку и необходимые работы по совершенствованию информационного, математического, методического, метрологического, организационного, программного, технического и иных видов обеспечения системы.

[ГОСТ Р 59356—2021, пункт 3.1.38]

3.30

существенная угроза (для нарушения интероперабельности системы): Угроза, при реализации которой риск нарушения требуемой интероперабельности системы превышает задаваемый допустимый уровень.

[Адаптировано из ГОСТ Р 50922—2006, пункт 2.6.1]

3.31

существенное условие (для нарушения интероперабельности системы): Критичное для обеспечения интероперабельности системы условие в контексте использования системы, при осуществлении которого риск нарушения требуемой интероперабельности системы превышает задаваемый допустимый уровень.

[Адаптировано и скомплексировано из ГОСТ Р ИСО/МЭК 25000—2021, пункт 4.2 и ГОСТ Р 50922—2006, пункт 2.6.1]

3.32

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

[ГОСТ Р 59194—2020, пункт 3.1.21]

3.33

угроза (для нарушения интероперабельности системы): Совокупность обстоятельств и факторов, создающих потенциальную или реально существующую опасность нарушения требуемой интероперабельности системы.

[Адаптировано из ГОСТ Р 50922—2006, пункт 2.6.1]

3.34

условие использования системы (критичное для обеспечения интероперабельности системы): Физическое и/или логическое условие, необходимое для обеспечения требуемой интероперабельности при использовании системы по назначению.

Примечание — Условия использования системы определяются допустимыми количественными значениями, при необходимости — с указанием диапазонов допустимых отклонений.

[Адаптировано из ГОСТ 33707—2016, статья 4.1443]

3.35

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

[ГОСТ Р 59341—2021, пункт 3.1.31]

4 Общие положения

4.1 В настоящем стандарте рассматриваются системы различного функционального назначения, создаваемые человеком для любой области приложений. Например, это могут быть системы в интересах органов государственной власти и корпораций, энергетических и промышленных структур (в том числе для отдельных предприятий, строительных, нефтегазовых и транспортных комплексов, опасного производства), предприятий оборонно-промышленного комплекса, атомной промышленности, служб по чрезвычайным ситуациям, информационно-управляющие системы, системы с использованием технологий искусственного интеллекта и другие. При этом под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей.

4.2 Важное практическое значение для эффективного взаимодействия различных систем (подсистем, компонентов, элементов систем) имеет свойство интероперабельности, характеризующее способность двух или более систем или компонентов к обмену необходимой информацией и к использованию информации, полученной в результате такого обмена. Пример проблемно-ориентированного описания интероперабельности системы с учетом положений ГОСТ Р 55062, ГОСТ Р 59797, ГОСТ Р 70569 представлен на рисунке 1 с условным выделением организационного, семантического и технического уровней.

В рамках настоящего стандарта системный анализ интероперабельности применяется для решения задач определения существенных угроз и условий, способных при том или ином развитии событий негативно или позитивно повлиять на качество, безопасность, эффективность и прогнозируемые риски относительно двух и более рассматриваемых систем. Возможно рассмотрение интероперабельности одной конкретной системы, условно предполагая ее сравнение с некоторой системой-эталоном или системой-аналогом.

Результаты определения существенных угроз и условий подлежат использованию при решении задач системной инженерии, включая обоснование мер, направленных на эффективное противодействие угрозам и поддержание приемлемых условий использования систем в условиях ограничений на задаваемые допустимые риски, а также правовых, функциональных, нормативно-технических, технологических, климатических, экологических и иных ограничений (в том числе на природные, временные, стоимостные, людские, технические ресурсы).

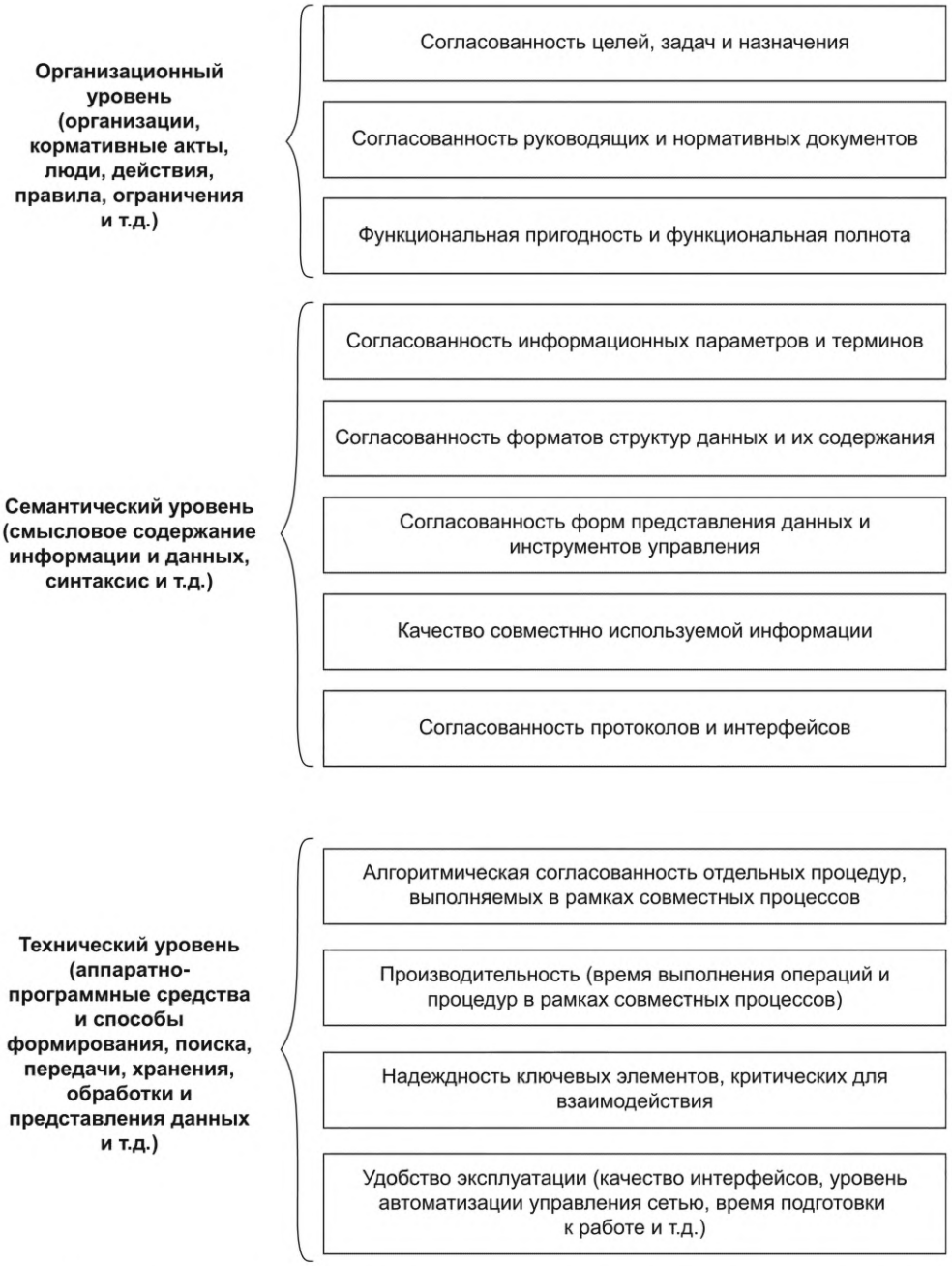

Рисунок 1 — Пример проблемно-ориентированного описания интероперабельности системы

4.3 Определение существенных угроз и условий, способных при том или ином развитии событий негативно или позитивно повлиять на интероперабельность рассматриваемой системы (подсистемы или системного элемента), выполняют с использованием методов системного анализа специальных показателей интероперабельности, связанных с критичными сущностями рассматриваемой системы, в том числе с помощью методов прогнозирования рисков. При этом используемые методы определения существенных угроз и условий должны быть целенаправлены на раннее распознавание и оценку развития предпосылок к нарушению качества, безопасности и/или эффективности рассматриваемой системы.

4.4 Для определения существенных угроз и условий при наличии достаточных фактических данных, позволяющих пренебречь условиями неопределенности, используют результаты измерений и оценок специальных показателей, связанных с критичными сущностями рассматриваемой системы и характеризующих нарушение качества, безопасности и/или эффективности (проявляющиеся как следствие нарушения интероперабельности рассматриваемой системы).

4.5 Для определения существенных угроз и условий при отсутствии или недостаточности фактических данных, а также при необходимости учета различных неопределенностей на задаваемый период прогноза рассматриваемая система формально представляется в виде моделируемой системы. Для выбранных показателей рисков устанавливают допустимые риски, выражаемые в виде количественных ограничений с возможными дополнительными логическими требованиями. При этом рассматривают следующие риски:

- риск нарушения интероперабельности как таковой (без учета дополнительных специфических требований к системе, например требований по защите информации);
- риск нарушения дополнительных специфических требований к системе;
- интегральный риск нарушения качества, безопасности и/или эффективности, учитывающий нарушения интероперабельности рассматриваемой моделируемой системы.

Примечание — В общем случае количественные ограничения на допустимые риски, устанавливаемые для решения задач определения существенных угроз и условий, могут отличаться от количественных ограничений на допустимые риски, устанавливаемые для решения других задач, например задач поддержки принятия решений по обеспечению эффективности рассматриваемой системы в ее ЖЦ. Подобные отличия обусловлены различными целями решения разных задач.

4.6 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, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р 59989, ГОСТ Р 59990, ГОСТ Р 59991, ГОСТ Р 59992, ГОСТ Р 59993, ГОСТ Р 59994, ГОСТ Р 71998 с учетом специфики системы и реализуемой стадии ее ЖЦ.

5 Рекомендации по определению существенных угроз и условий

5.1 При решении задач системной инженерии, позволяющих пренебречь последствиями неопределенности, для определения существенных угроз и условий составляют полный перечень угроз нарушения интероперабельности системы и условий использования системы, критичных с точки зрения обеспечения ее интероперабельности. Каждой угрозе и каждому условию сопоставляют соответствующие последствия от реализации этих угроз и условий. Сопоставляемые последствия характеризуют потенциальный ущерб от нарушения интероперабельности и могут быть выражены как качественно (например, «недопустимый ущерб», «большой ущерб» с использованием логических описаний последствий или «допустимый ущерб»), так и количественно (например, ущерб в рублях, часах неработоспособности или в каких-либо иных условных единицах). Причем как в качественном, так и в количественном выражениях фиксируют состояния, признаваемые с точки зрения интероперабельности как недопустимые, остальные уровни признают допустимыми, т. е. приемлемыми для практического использования. Это вырожденный случай, который возможен именно в силу пренебрежения условиями неопределенности. На практике случается редко — например, это могут быть автоматические системы, которые предназначены для совместной работы в стабильных условиях в течение длительных периодов эксплуатации независимо от контроля человека (например, автоматические сенсорные устройства в газопроводе, обменивающиеся информацией с контрольно-диспетчерским пунктом с использованием технологий искусственного интеллекта).

В рамках составленного полного перечня угроз и условий используют следующие критерии:

- угрозу нарушения интероперабельности системы признают существенной, если установленное для нее множество возможных последствий признано недопустимым;
- условие использования системы, критичное для обеспечения ее интероперабельности, признают существенным, если при осуществлении этого условия множество возможных последствий признано недопустимым.

Ранжирование существенных угроз и условий проводится по необходимости, оно может быть осуществлено только в том случае, когда возможно сравнение последствий: чем последствия хуже, тем опасность соответствующих угроз и условий выше.

5.2 При решении задач системной инженерии, когда пренебречь условиями и последствиями неопределенности невозможно (это наиболее распространенный случай), для определения существенных угроз и условий составляют изначальный возможный перечень угроз нарушения интероперабельности и условий использования системы, критичных с точки зрения обеспечения интероперабельности системы. При необходимости этот перечень может расширяться и уточняться во времени и по содержанию, в том числе из-за изменения условий неопределенности.

Для определения существенных угроз и условий используют математические методы прогнозирования рисков применительно к моделируемой системе в задаваемый период прогноза (см. ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р 59989, ГОСТ Р 59990, ГОСТ Р 59991, ГОСТ Р 59992, ГОСТ Р 59993, ГОСТ Р 59994, ГОСТ Р 71998). Используют следующие критерии:

- угрозу нарушения интероперабельности системы признают существенной, если для нее прогнозное значения риска (см. 4.5) превышает установленное значение соответствующего допустимого риска (при сопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы) и/или математическое ожидание ущерба превышает установленный допустимый уровень (при несопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы);
- условие использования системы, критичное для обеспечения ее интероперабельности, признают существенным, если при осуществлении этого условия прогнозное значение риска превышает установленное значение допустимого риска (при сопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы) и/или математическое ожидание ущерба превышает установленный допустимый уровень (при несопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы).

Непревышение допустимого риска на вероятностном уровне или на уровне математического ожидания ущерба интерпретируют как несущественность рассматриваемых угроз и соблюдение условий по удержанию риска в допустимых пределах в течение периода прогноза.

Если в приложении к моделируемой системе все расчетные риски не превышают установленных допустимых рисков, это означает, что результаты моделирования подтверждают удержание рисков в допустимых пределах, т. е. существенные угрозы и условия для системы в течение периода прогноза считают отсутствующими. Если какие-то расчетные риски превышают максимально допустимые, это означает уязвимость рассматриваемой системы с точки зрения нарушения ее интероперабельности для соответствующих угроз и условий, которые, в свою очередь, характеризуются как существенные.

Ранжирование существенных угроз и условий проводят по необходимости, оно может быть осуществлено лишь в случае, когда возможно количественное сравнение последствий (например, в условных единицах).

При сопоставимых ущербах применим следующий критерий: чем вероятностное выражение риска выше, тем более высокой считают опасность соответствующих угроз и условий (в этом случае достаточно ограничиться сравнением на вероятностном уровне). В свою очередь, при несопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы необходим учет различных последствий нарушения интероперабельности. В этом случае применим следующий критерий: чем выше значение математического ожидания ущерба в задаваемый период прогноза, тем более высокой считают опасность соответствующих угроз и условий в этот период.

Примечание — Результат произведения вероятностного значения прогнозируемого риска в задаваемый период прогноза на количественное значение потенциального ущерба может быть интерпретирован как математическое ожидание ущерба. Тем самым для одинаковых единиц измерения ранжирование существенных угроз и условий проводят по шкале математического ожидания ущерба в единицах количественного измерения последствий нарушения интероперабельности.

5.3 Для прогнозирования рисков на практике могут быть использованы любые научно обоснованные формализованные модели и методы, обеспечивающие достижение целей и решение поставленных задач системного анализа интероперабельности (см. ГОСТ Р 59991).

Примеры формализации для прогнозирования рисков при определении существенных угроз и явлений приведены в приложении А.

Приложение А
(справочное)

Примеры формализации для прогнозирования рисков при определении существенных угроз и явлений

А.1 Согласно 4.4 и 5.1 случай определения существенных угроз и условий, характеризуемый наличием достаточных фактических данных, позволяющих пренебречь условиями неопределенности, не требует каких-либо специальных математических моделей и методов для прогнозирования рисков. Достаточно применения подходов, изложенных в 4.4 и 5.1.

Примечание — В этом случае, характеризуемом полной предсказуемостью, понятие риска как меры опасности для оценки влияния неопределенности на достижение поставленных целей теряет свою содержательность. Существенность угроз и условий является полностью определяемой по установленной тяжести возможных последствий от нарушения интероперабельности.

А.2 В общем случае учета неопределенностей для прогнозирования рисков нарушения интероперабельности рассматриваемые примеры математических моделей и методов, как показано на рисунке А.1, ориентированы на типовую архитектуру системы (см. также ГОСТ Р 59797).

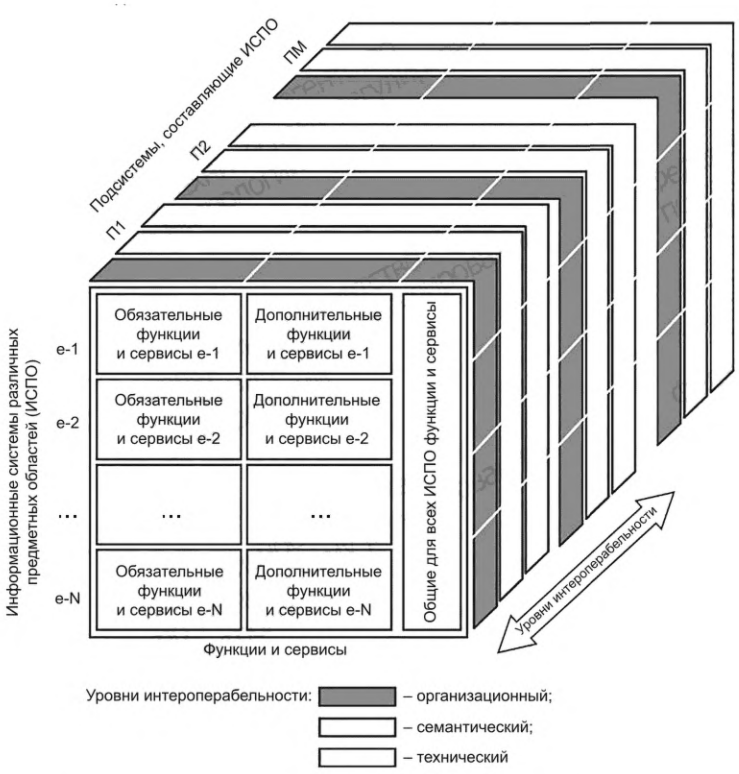

Рисунок А.1 — Типовая архитектура системы с точки зрения интероперабельности (по ГОСТ Р 59797)

Далее в А.3 — А.7 приведены описания и ссылки на математические модели и методы, обеспечивающие прогнозирование рисков в целях определения существенных угроз и условий согласно положениям 4.5 и 5.2. Примеры возможных угроз и условий приведены в приложении Б.

Математические модели и методы, рекомендуемые в настоящем приложении, учитывают требования и методические подходы в соответствии с положениями ГОСТ Р ИСО/МЭК 33002, ГОСТ Р ИСО/МЭК 33003, ГОСТ Р ИСО/МЭК 33004, ГОСТ Р 57193, ГОСТ Р 58606, ГОСТ Р 58771, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р 59989, ГОСТ Р 59990, ГОСТ Р 59991, ГОСТ Р 59992, ГОСТ Р 59993, ГОСТ Р 59994, ГОСТ Р МЭК 61069-1, 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 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62508, ГОСТ Р 71303, ГОСТ Р 71438, ГОСТ Р 71440, ГОСТ Р 71998.

А.3 С точки зрения системного анализа в качестве оцениваемых выступает моделируемая система, представляющая собой формализованную модель рассматриваемой системы и формализованные модели учитываемых сущностей качества информации в условиях применения системы. Получаемые в результате моделирования результаты прогнозирования рисков и решения прикладных задач распространяются на рассматриваемую систему.

Основной целью прогнозирования рисков для моделируемой системы является установление степени вероятного нарушения требований по обеспечению интероперабельности за период прогноза (для упрощения последствия применительно к различным типам информации и расчетным показателям на семантическом уровне полагаются сравнимыми). Цель может варьироваться в зависимости от периода прогноза и контекста предполагаемого использования моделируемой системы.

Целеполагание при прогнозировании рисков нарушения интероперабельности позволит количественно решать следующие прикладные задачи системного анализа (см. ГОСТ Р 59991):

- прогнозирование рисков, интерпретации и анализ получаемых результатов, включая сравнение прогнозируемых значений оцениваемых показателей с допустимым уровнем на предмет выполнения задаваемых ограничений;
- обоснование допустимых рисков;
- определение существенных угроз и условий, способных при том или ином развитии событий в ЖЦ негативно или позитивно повлиять на свойства, способных недопустимо ухудшить качество и/или безопасность и/или эффективность рассматриваемой моделируемой системы;
- определение и обоснование в ЖЦ моделируемой системы упреждающих мер противодействия угрозам и условий снижения рисков или удержания рисков в допустимых пределах, обеспечивающих желаемый уровень интероперабельности для рассматриваемой системы при задаваемых ограничениях в период прогноза;
- обоснование рекомендаций по минимизации рисков нарушения интероперабельности моделируемой системы с учетом дополнительных специфических требований (например, требований по защите информации).

А.4 Для математической формализации приняты следующие предположения:

- возникновение и развитие различных угроз и условий, критичных для обеспечения интероперабельности системы в условиях неопределенностей, описывается в терминах случайных событий;
- для различных вариантов развития угроз нарушения интероперабельности средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность контрмер, предназначенных для преодоления барьеров интероперабельности и воспрепятствования реализации угроз и/или ухудшению условий использования моделируемой системы;
- в общем случае в моделируемой системе интероперабельность на семантическом уровне (см. ГОСТ Р 59341) зависит от своевременности предоставления используемой информации, полноты оперативного отражения в системе новых объектов и явлений, актуальности обновляемой информации, безошибочности информации после контроля, корректности обработки информации, обеспечения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации);
- к началу периода прогноза целостность моделируемой системы обеспечена, включая изначальное выполнение требований по обеспечению интероперабельности.

Предупреждающие контрмеры характеризуются обоснованным использованием выбранных мер противодействия угрозам (и/или удержания в допустимых пределах условий, критичных для обеспечения интероперабельности). Дополнительно делают предположение о наличии возможностей по определению предпосылок к реализации угроз (и/или к ухудшению критичных условий использования системы), наличии мер противодействия угрозам (и/или удержания в допустимых пределах критичных условий использования системы), наличии способов выявления последствий следов реализации угроз (и/или последствий проявления критичных условий в недопустимых пределах), а также наличии возможностей по приемлемому восстановлению нарушаемых условий функционирования моделируемой системы с точки зрения обеспечения ее интероперабельности.

А.5 Для определения существенных угроз и явлений могут быть использованы математические модели и методы прогнозирования рисков, изложенные в ГОСТ Р 59341, ГОСТ Р 59991 и ГОСТ Р 59994. Поэтому далее приведены ссылки на соответствующие положения в указываемых стандартах. Рекомендуемые показатели поддерживаются математическими моделями и методами, обеспечивающими проведение оценок различных рисков и прогнозирование интегрального риска нарушения интероперабельности моделируемой системы. Частные показатели учитывают возможные нарушения интероперабельности подсистем в их ЖЦ на организационном, семантическом и техническом уровнях (см. рисунок А.1).

Для прогнозирования рисков при сопоставимых последствиях рекомендуются следующие количественные показатели:

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на организационном уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это частный показатель;

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на семантическом уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это частный показатель.

Примечание — Для многосторонних научно-практических исследований необходимо учитывать, что в общем случае интероперабельность в моделируемой системе на семантическом уровне будет зависеть от своевременности предоставления используемой информации, полноты оперативного отражения в системе новых объектов и явлений, актуальности обновляемой информации, безошибочности информации после контроля, корректности обработки информации, обеспечения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации);

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на техническом уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это частный показатель;
- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на организационном уровне при выполнении дополнительных функций и сервисов в течение заданного периода прогноза. Это частный показатель;
- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на семантическом уровне при выполнении дополнительных функций и сервисов путем анализа задаваемого объема информации. Это частный показатель;
- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на техническом уровне при выполнении дополнительных функций и сервисов в течение заданного периода прогноза. Это частный показатель;
- интегральный риск нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза (на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов). Это интегральный показатель, учитывающий дополнительные расчетные показатели в зависимости от индикаторных условий (α) и вероятностных значений частных показателей, определенных выше (см. соответствующие условия α из ГОСТ Р 59341—2021, приложение В, В.3.2—В.3.8, а также приложение А, А.6.4).

А.6 В условиях неопределенности для оценки частных и интегрального рисков нарушения интероперабельности моделируемой системы из А.5 далее применяются математические модели, рекомендованные ГОСТ Р 59341, ГОСТ Р 59991 и ГОСТ Р 59994. Применяемые модели ориентированы на возможные угрозы нарушения интероперабельности системы и условия использования системы, критичные с точки зрения обеспечения ее интероперабельности (см. приложение Б).

А.6.1 Для оценки риска нарушения интероперабельности в моделируемой системе на организационном уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза применяют модели для оценки безошибочности действий пользователей и персонала системы (см. ГОСТ Р 59341—2021, приложение В, В.3.8). В качестве исходных данных для расчетов выступают:

σ — частота возникновения источников угроз с точки зрения нарушения интероперабельности на организационном уровне;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий пользователей и персонала);

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

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

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы;

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

В общем случае такие исходные данные, как $T_{меж}$ и $T_{диаг}$, на практике определяют в руководствах по контролю целостности системы или путем измерений. В свою очередь, для определения σ, β, $T_{восст}$ рекомендуется использование универсальной вспомогательной модели показателя (УВМП) (см. ГОСТ Р 59349). Значения σ, β, $T_{восст}$, получаемые по результатам анализа данных мониторинга (или пересчета этих параметров на уровне УВМП), являются исходными данными для формального описания моделируемой системы с учетом возможности прогнозирования динамики разнородных событий. В общем случае показатель УВМП может быть использован при формировании исходных данных и применении моделей для семантического и технического уровней интероперабельности.

А.6.2 Для оценки риска нарушения интероперабельности в моделируемой системе на семантическом уровне при выполнении обязательных и дополнительных функций и сервисов применяют различные частные показатели, призванные охарактеризовать качество используемой информации в системе с помощью математических моделей:

1) для оценки своевременности предоставления используемой информации применяют модели для оценки своевременности предоставления информации (см. ГОСТ Р 59341—2021, приложение В, В.3.3), где используют исходные данные для расчетов T_i и $|(T_i^2 - T_{i2})|^{0,5}$ — соответственно среднее время и среднеквадратичное отклоне-

ние времени реакции системы при обработке запросов *i*-го типа (т. е. полного времени пребывания на обработке с учетом ожидания в очередях), T_{i2} — второй момент времени реакции. Как правило, в качестве исходных данных формируют целиком именно среднеквадратичное отклонение, не опускаясь до отдельных измерений второго момента. Для каждого из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) требования к своевременности обработки запросов в системе (касающиеся как запрашиваемой, так и выдаваемой принудительно информации) указывают в виде одного из двух критериев:

- критерий своевременности по среднему времени реакции: среднее время обработки запросов *i*-го типа T_i должно быть не более задаваемого $T_{зад\ i}$ (далее условие этого критерия упоминается как условие своевременности α_1);

- вероятностный критерий: вероятность своевременной обработки запросов *i*-го типа в системе $P_{св\ i}(T_{зад\ i}) = P_{св\ i}(\tau_i \le T_{зад\ i})$ за заданное время $T_{зад\ i}$ должна быть не ниже задаваемой $P_{св\ зад\ i}$ (далее условие этого критерия упоминается как условие своевременности α_2), где τ_i — случайная величина, означающая время реакции системы при обработке запросов *i*-го типа;

2) для оценки полноты оперативного отражения в системе новых объектов и явлений применяют модели для оценки полноты оперативного отражения в системе новых объектов и явлений (см. ГОСТ Р 59341—2021, приложение В, В.3.4), где используются исходные данные для расчетов:

λ — частота появления новых объектов и явлений в процессе функционирования системы;

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода новых объектов учета в базу данных (БД) системы;

3) для оценки актуальности обновляемой информации применяют модели для оценки актуальности обновляемой информации (см. ГОСТ Р 59341—2021, приложение В, В.3.5), где используются исходные данные для расчетов:

ξ — среднее время между значимыми изменениями реальной информации относительно информации, хранимой в системе (т. е. ξ^{-1} — частота значимого изменения);

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода в БД данных от источников информации;

q — среднее время между соседними обновлениями данных (т. е. q^{-1} — частота обновления данных) в системе при обновлении ее по регламенту;

4) для оценки безошибочности информации после контроля применяют модели для оценки безошибочности информации после контроля (см. ГОСТ Р 59341—2021, приложение В, В.3.6), где используются исходные данные для расчетов:

V — объем контролируемой информации;

μ — доля первоначальных ошибок в контролируемой информации в объеме V (до контроля), т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν — средняя скорость контроля информации;

n — частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки);

$T_{нар}$ — среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной (для программно-технических средств — это время наработки на отказ);

$T_{непр}$ — период непрерывной работы контролера;

$T_{зад}$ — задаваемое время на контроль информации;

5) для оценки корректности обработки информации применяют модели для оценки корректности обработки информации (см. ГОСТ Р 59341—2021, приложение В, В.3.7), где используются исходные данные для расчетов:

V — объем информации, подлежащий обработке (анализу);

μ — часть важной для принятия решения информации, которая должна быть объективно использована при обработке (анализе) информации объема V, т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν — скорость обработки (анализа);

n — частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной);

$T_{нар}$ — среднее время наработки на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это — аналог ошибки контроля 2-го рода);

$T_{непр}$ — период непрерывной работы аналитика (в качестве аналитика могут выступать программно-математические средства или пользователь системы);

$T_{зад}$ — задаваемое время на обработку (анализ) информации;

6) для оценки безопасности информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий применяют модели для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий (см. ГОСТ Р 59341—2021, приложение В, В.3.9.2), где используются исходные данные для расчетов:

σ — частота возникновения источников угроз в виде источников опасных программно-технических воздействий на моделируемую систему;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса или защищаемых активов, используемых при выполнении действия) в результате опасных программно-технических воздействий;

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

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

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы;

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

7) для оценки безопасности информации в части защищенности активов от несанкционированного доступа применяют модели для оценки защищенности активов от несанкционированного доступа (см. ГОСТ Р 59341—2021, приложение В, В.3.9.3), где используются исходные данные для расчетов:

M — количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

f_m — среднее время между соседними изменениями параметров защиты m-й преграды;

u_m — среднее время преодоления (вскрытия значений параметров защиты) m-й преграды;

8) для оценки безопасности информации в части сохранения конфиденциальности используемой информации применяют модели для оценки сохранения конфиденциальности используемой информации (см. ГОСТ Р 59341—2021, приложение В, В.3.9.3), где используются исходные данные для расчетов:

M — количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

f_m — среднее время между соседними изменениями параметров защиты m-й преграды;

u_m — среднее время преодоления (вскрытия значений параметров защиты) m-й преграды;

$T_{конф}$ — период объективной конфиденциальности используемой информации.

А.6.3 Для оценки риска нарушения интероперабельности в моделируемой системе на техническом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза применяют модель для оценки надежности предоставления информации (см. ГОСТ Р 59341—2021, приложение В, В.3.2), модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий (см. ГОСТ Р 59341—2021, приложение В, В.3.9.2) (для программно-технических аспектов, влияющих на интероперабельность). В качестве исходных данных для расчетов выступают:

σ — частота возникновения источников угроз с точки зрения нарушения интероперабельности на техническом уровне;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы с точки зрения нарушения интероперабельности на техническом уровне;

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

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

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы;

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

Примечание — Несмотря на фактическую повторяемость некоторых названий исходных данных (поскольку используются одни и те же модели), их значения при моделировании при выполнении дополнительных функций и сервисов, возможно, будут отличаться от количественных значений этих исходных данных при выполнении обязательных функций и сервисов, а также в сравнении с организационным и семантическим уровнями, поскольку различны их природа, причины формирования значений, интерпретация и области приложений. С учетом различий соответственно разными будут и расчетные риски.

А.6.4 В качестве исходных данных для оценки интегрального риска нарушения интероперабельности моделируемой системы в течение заданного периода прогноза (на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов) используют расчетные показатели, рассчитываемые с помощью моделей А.6.1—А.6.3 по алгоритму расчета интегрального риска нарушения реализации процесса с учетом требований по защите информации (см. ГОСТ Р 59341—2021, приложение В, В.3.10), где используются показатели:

$Z_{над\ предст}(T_{зад})$ — вероятностный коэффициент надежности предоставления информации, учитывающий вероятность надежного предоставления информации в системе в течение заданного периода прогноза $T_{зад}$ и соответствующие условия α (определение коэффициента см. ГОСТ Р 59341—2021, приложение В, В.3.2);

$Z_{своевр}$ — вероятностный коэффициент своевременности обработки запросов, учитывающий относительную долю своевременно обработанных в системе запросов и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.3);

$Z_{полн}$ — вероятностный коэффициент полноты оперативного отражения в системе новых объектов и явлений, учитывающий вероятность того, что в системе полностью отражены состояния всех реально суще-

ствующих критичных объектов и явлений, и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.4);

$Z_{акт}$ — вероятностный коэффициент актуальности информации в системе, учитывающий вероятность сохранения актуальности информации на момент ее использования и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.5);

$Z_{безош}$ — вероятностный коэффициент безошибочности информации в системе, учитывающий вероятность отсутствия ошибок в информации после ее контроля и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.6);

$Z_{корр}$ — вероятностный коэффициент корректности обработки информации в системе, учитывающий вероятность получения корректных результатов обработки информации и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.7);

$Z_{чел}$ ($T_{зад}$) — вероятностный коэффициент безошибочных действий пользователей и персонала системы, учитывающий вероятность безошибочных действий пользователей и персонала в течение заданного периода прогноза и соответствующие условия α (определение коэффициента см. в ГОСТ Р 59341—2021, приложение В, В.3.8);

$P_{возд}(T_{зад})$ — вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $T_{зад}$ (определение по рекомендациям см. в ГОСТ Р 59341—2021, приложение В, В.3.9.2);

$P_{НСД}$ ($T_{зад}$) — вероятность обеспечения защищенности активов системы от НСД в течение заданного периода прогноза $T_{зад}$ (или без привязки к этому периоду — $P_{НСД}$) (определение по рекомендациям см. в ГОСТ Р 59341—2021, приложение В, В.3.9.3);

$P_{конф}(T_{конф})$ — вероятность сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $T_{конф}$ (определение по рекомендациям см. в ГОСТ Р 59341—2021, приложение В, В.3.9.4), период $T_{конф}$ может играть роль периода прогноза $T_{зад}$ (см. ГОСТ Р 59341—2021, приложение В, В.3.9.4).

А.7 Интегральный риск используется для сравнения весомости прогнозируемых частных рисков, выявления существенных угроз и условий и поддержки принятия решений для задач системного анализа при разработке и эксплуатации системы в сопоставлении с возможным ущербом. Например, интегральный риск нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов $R_{интегр}$ ($T_{зад}$) для прогнозного периода $T_{зад}$ согласно А.3—А.6 может быть определен по формуле

$$R_{интегр}\,(T_{зад}) = 1 - [1 - R_{наруш}\,(T_{зад})]\,[1 - R_{надежн}\,(T_{зад})]; \quad (А.1)$$

где $R_{наруш}$ ($T_{зад}$) — риск нарушения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации) в течение периода прогноза $T_{зад}$. Показатель $R_{наруш}$ ($T_{зад}$) относится к семантическому уровню интероперабельности и может быть рассчитан по моделям и рекомендациям А.6

$$R_{наруш}\,(T_{зад}) = 1 - P_{возд}\,(T_{зад}) \cdot P_{НСД}\,(T_{зад}) \cdot P_{конф}(T_{конф}); \quad (А.2)$$

$R_{надежн}$ ($T_{зад}$) — обобщенный виртуальный показатель для организационного, семантического и технического уровней, учитывающий в течение задаваемого периода прогноза $T_{зад}$ надежность и своевременность предоставления используемой информации, полноту оперативного отражения в системе новых объектов и явлений, актуальность обновляемой информации, безошибочность информации после контроля, корректность обработки информации и безошибочность действий пользователей и персонала системы. Этот виртуальный показатель для моделируемой системы может быть рассчитан по моделям и рекомендациям А.3—А.6

$$R_{надежн}\,(T_{зад}) = 1 - Z_{над\ предст}(T_{зад}) \cdot Z_{своевр} \cdot Z_{полн} \cdot Z_{акт} \cdot Z_{безош} \cdot Z_{корр.} \cdot Z_{чел}(T_{зад}). \quad (А.3)$$

Здесь к организационному уровню интероперабельности относится $Z_{чел}(T_{зад})$, к семантическому уровню — показатели $Z_{своевр}$, $Z_{полн}$, $Z_{акт}$, $Z_{безош}$, $Z_{корр,}$ а также $P_{возд}\,(T_{зад}) \cdot P_{НСД}\,(T_{зад}) \cdot P_{конф}(T_{конф})$, к техническому уровню — $Z_{над\ предст}(T_{зад})$.

При этом на организационном уровне интероперабельности для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{доп.\ чел}\,(T_{зад})$ и условие α. При этом условие α касается безошибочности действий пользователей и персонала системы и формулируется в виде ограничений: $P_{чел}\,(T_{зад}) \geq P_{доп.\ чел}\,(T_{зад})$ и возможный ущерб от нарушения интероперабельности не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочных действий пользователей и персонала системы $Z_{чел}\,(T_{зад})$

$$Z_{чел}(T_{зад}) = \begin{cases} 1, \text{ если условие безошибочности действий } \alpha \text{ выполнено,} \\ P_{чел}(T_{зад}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

На семантическом уровне интероперабельности для оценки своевременности предоставления информации используют вспомогательное понятие относительной доли своевременно обработанных в системе запросов $C_{\text{своевр}}$. Этот вспомогательный показатель охватывает лишь те типы запросов, для которых выполнены требования потребителя информации, этот показатель вычисляют по формуле

$$C_{\text{своевр}} = \sum_{i=1}^{I} \lambda_i P_{\text{св}\,i}(T_{\text{зад}\,i})[Ind(\alpha_1) + Ind(\alpha_2)] / \sum_{i=1}^{I} \lambda_i, \qquad \text{(A.4)}$$

где λ_i — частота поступления на обработку запросов i-го типа.

Критерии своевременности обработки каждого типа запросов устанавливают с использованием индикаторной функции $Ind\,(\alpha)$:

$$Ind(\alpha) = \begin{cases} 1, \text{ если условие } \alpha \text{ истинно,} \\ 0, \text{ если условие } \alpha \text{ ложно.} \end{cases}$$

При этом для i-го типа запросов условие своевременности α с учетом возможных ущербов определяют одним из условий, α_1 или α_2:

- α_1 — условие, когда для i-го типа запросов задан критерий своевременности по среднему времени реакции и $T_i \le T_{\text{зад}\,i}$;
- α_2 — условие, когда для i-го типа запросов задан вероятностный критерий своевременности и $P_{\text{св}\,i}(\tau_i \le T_{\text{зад}\,i}) \ge P_{\text{св зад}\,i}$.

Для оценки интегрального риска условие своевременности предоставления информации α формулируют в виде условий α_1 или α_2 для каждого i-го типа запросов с добавлением, что в случае их нарушения возможный ущерб не превышает допустимого (это формулировка условия α по всем типам запросов). Учет результатов моделирования осуществляют с использованием индикаторного коэффициента своевременности обработки запросов $Z_{\text{своевр}}$

$$Z_{\text{своевр}} = \begin{cases} 1, \text{ если условия своевременности } \alpha \text{ выполнены для всех типов запросов,} \\ C_{\text{своевр}} \text{ по (А.4), если хотя бы одно условие не выполнено.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп полн}}$ и условие α. При этом условие α касается полноты оперативного отражения в системе новых объектов и явлений и формулируется в виде ограничений $P_{\text{полн}} \ge P_{\text{доп. полн}}$, и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием вероятностного коэффициента полноты оперативного отражения в системе новых объектов и явлений $Z_{\text{полн}}$

$$Z_{\text{полн}} = \begin{cases} 1, \text{ если условие полноты отражения в системе объектов и явлений } \alpha \text{ выполнено,} \\ P_{\text{полн}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп. акт}}$ и условие α. При этом условие α касается сохранения актуальности информации в системе на момент ее использования и формулируется в виде ограничений $P_{\text{акт}} \ge P_{\text{доп. акт}}$, и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента актуальности информации в системе $Z_{\text{акт}}$

$$Z_{\text{акт}} = \begin{cases} 1, \text{ если условие сохранения актуальности информации в системе } \alpha \text{ выполнено,} \\ P_{\text{акт}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп. безош}}$ и условие α. При этом условие α касается обеспечения безошибочности информации после контроля и формулируется в виде ограничений $P_{\text{безош}} \ge P_{\text{доп. безош}}$, и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочности информации в системе $Z_{\text{безош}}$

$$Z_{\text{безош}} = \begin{cases} 1, \text{ если условие безошибочности информации после контроля } \alpha \text{ выполнено,} \\ P_{\text{безош}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп. корр}}$ и условие α. При этом условие α касается обеспечения корректности обработки информации и формулируется в виде ограничений $P_{\text{корр}} \ge P_{\text{доп. корр}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента корректности обработки информации в системе $Z_{\text{корр}}$

$$Z_{\text{корр}} = \begin{cases} 1, \text{ если условие обеспечения корректности обработки информации } \alpha \text{ выполнено,} \\ P_{\text{корр}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

На техническом уровне интероперабельности для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп. над}}(T_{\text{зад}})$ и условие α. При этом условие α касается надежности предоставления информации и формулируется в виде ограничений $P_{\text{над. предст}}(T_{\text{зад}}) \geq P_{\text{доп. над}}(T_{\text{зад}})$, и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента надежности предоставления информации $Z_{\text{над. предст}}(T_{\text{зад}})$

$$Z_{\text{над.предст}}(T_{\text{зад}}) = \begin{cases} 1, \text{ если условие надежности предоставления информации } \alpha \text{ выполнено,} \\ P_{\text{над.предст}}(T_{\text{зад}}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы произведения упомянутых коэффициентов $(1 - Z_{\ldots})$ в качестве вероятностного выражения соответствующего риска.

Примечания

1 Другие возможные показатели, модели, методы и рекомендации по оценке рисков см. в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-1, ГОСТ Р МЭК 61069-2, 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 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7.

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

Приложение Б
(справочное)

Примеры возможных угроз и условий

Б.1 Перечень возможных угроз нарушения интероперабельности системы может включать:

- природные и природно-техногенные угрозы (см. ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7);
- угрозы со стороны человеческого фактора (см. ГОСТ Р МЭК 62508);
- угрозы безопасности информации, качеству и безопасности функционирования программного обеспечения, оборудования и коммуникаций, используемых в процессе работы (см. ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 51583, ГОСТ Р 54124, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р 59989, ГОСТ Р 59990, ГОСТ Р 59991, ГОСТ Р 59992, ГОСТ Р 59993, ГОСТ Р 59994);
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) (см. ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С);
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (изготовителя) к конкретному заказчику, системы которого были скомпрометированы;
- прочие соответствующие угрозы качеству, безопасности и эффективности системы, связанные с нарушением интероперабельности на организационном, семантическом или техническом уровнях при выполнении обязательных и дополнительных функций и сервисов в системе (см. ГОСТ Р 59989, ГОСТ Р 59990, ГОСТ Р 59991, ГОСТ Р 59992, ГОСТ Р 59993, ГОСТ Р 59994, ГОСТ Р МЭК 61069-1, 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 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62508, ГОСТ Р 71303, ГОСТ Р 71438, ГОСТ Р 71440, ГОСТ Р 71998).

Б.2 Перечень возможных условий использования системы, критичных с точки зрения обеспечения ее интероперабельности, может включать условия, характеризующие такой контекст использования моделируемой системы, при котором расчетный риск не превышает задаваемого допустимого при прочих неизменных параметрах. Эти условия могут быть сформированы на основе решения обратных задач (см. Б.2.1—Б.2.8).

Б.2.1 Условия в части управления риском нарушения интероперабельности на организационном уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемого условия α (применяют модель по А.6.1):

- частота возникновения источников угроз с точки зрения нарушения интероперабельности на организационном уровне σ не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий пользователей и персонала) β должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время системной диагностики целостности моделируемой системы $T_{диаг}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время восстановления нарушаемой целостности моделируемой системы $T_{восст}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого.

Б.2.2 Условия в части управления рисками нарушения интероперабельности на семантическом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемых условий α (применяют модели по А.6.2):

Б.2.2.1 Условия по А.6.2, перечисление 1), в части управления своевременностью предоставления используемой информации с помощью модели для оценки своевременности предоставления информации (см. ГОСТ Р 59341—2021, приложение В, В.3.3): частота поступления на обработку запросов i-го типа в системе, $i \geq 1$ (касающихся как запрашиваемой, так и выдаваемой принудительно информации), и среднее время их обработки для каждого из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) не должны превышать максимальных расчетных значений, влияющих на

расчетные значения T_i и $|(T_i^2 - T_{i2})|^{0,5}$, которые, в свою очередь, могут быть оценены на основе применения моделей массового обслуживания разнотипных запросов в системе и/или методом натурных испытаний, и/или имитационного моделирования), для которых при прочих неизменных исходных данных по каждому i-му типу запросов выполняется один из установленных критериев:

- критерий своевременности по среднему времени реакции: среднее время обработки запросов i-го типа T_i должно быть не более задаваемого $T_{зад\ i}$ (это условие своевременности α_1);

- вероятностный критерий: вероятность своевременной обработки запросов i-го типа в системе $P_{св\ i}(T_{зад\ i}) = P_{св\ i}(\tau_i \le T_{зад\ i})$ за заданное время $T_{зад\ i}$ должна быть не ниже задаваемой $P_{св.\ зад\ i}$ (это условие своевременности α_2), где τ_i — случайная величина, означающая время реакции системы при обработке запросов i-го типа.

Б.2.2.2 Условие по А.6.2, перечисление 2), в части управления полнотой оперативного отражения в системе новых объектов и явлений с помощью модели для оценки полноты оперативного отражения в системе новых объектов и явлений (см. ГОСТ Р 59341—2021, приложение В, В.3.4) (для каждого из различных типов информации): среднее время подготовки, передачи и ввода новых объектов учета в БД системы $T_{база\ данных}$ должно составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание — Необходимо учесть, что в реальности возможности влияния на частоту появления новых объектов и явлений в процессе функционирования системы λ практически отсутствуют.

Б.2.2.3 Условия по А.6.2, перечисление 3), в части управления актуальностью обновляемой информации с помощью модели для оценки актуальности обновляемой информации (см. ГОСТ Р 59341—2021, приложение В, В.3.5) (для каждого из различных типов информации):

- среднее время подготовки, передачи и ввода в БД данных от источников информации $T_{база\ данных}$ должно составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- частота обновления данных в системе при обновлении ее по регламенту q^{-1} должна составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание — Необходимо учесть, что в реальности возможности влияния на частоту значимого изменения реальной информации относительно информации, хранимой в системе ξ^{-1}, практически отсутствуют.

Б.2.2.4 Условия по А.6.2, перечисление 4), в части управления безошибочностью информации после контроля с помощью модели для оценки безошибочности информации после контроля (см. ГОСТ Р 59341—2021, приложение В, В.3.6) (для каждого из различных типов информации):

- объем контролируемой информации V должен составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- доля первоначальных ошибок в контролируемой информации в объеме V (до контроля — μ) должна составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- средняя скорость контроля информации ν должна быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки — n) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной $T_{нар}$, должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- период непрерывной работы контролера $T_{непр}$ не должен превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

- задаваемое время на контроль информации $T_{зад}$ должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание — Необходимо учесть, что в реальности возможности влияния на период непрерывной работы контролера $T_{непр}$ могут быть ограничены различными эргономическими требованиями.

Б.2.2.5 Условия по А.6.2, перечисление 5), в части управления корректностью обработки информации с помощью модели для оценки корректности обработки информации (см. ГОСТ Р 59341—2021, приложение В, В.3.7) (для каждого из различных типов информации):

- объем информации, подлежащий обработке или анализу V, должен составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- часть важной для принятия решения информации, которая должна быть объективно использована при обработке или анализе информации объема V (μ), должна составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- скорость обработки или анализа информации ν должна быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной — n) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- среднее время наработки на алгоритмическую ошибку, когда объективно важная для принятия решения информация игнорируется $T_{нар}$, должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- период непрерывной работы аналитика $T_{непр}$ не должен превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;
- задаваемое время на обработку или анализ информации $T_{зад}$ должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Б.2.2.6 Условие по А.6.2, перечисление 6), по управлению безопасностью информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий с помощью модели для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий (см. ГОСТ Р 59341—2021, приложение В, В.3.9.2):

- частота возникновения источников угроз в виде источников опасных программно-технических воздействий на моделируемую систему σ не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время развития угроз с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса или защищаемых активов, используемых при выполнении действия) в результате опасных программно-технических воздействий β должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время системной диагностики целостности моделируемой системы $T_{диаг}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время восстановления нарушаемой целостности моделируемой системы $T_{восст}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого.

Б.2.2.7 Условие по А.6.2, перечисление 7), по управлению безопасностью информации в части защищенности активов от несанкционированного доступа с помощью модели для оценки защищенности активов от несанкционированного доступа (см. ГОСТ Р 59341—2021, приложение В, В.3.9.3): количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы M, среднее время между соседними изменениями параметров защиты m-й преграды f_m и среднее время преодоления (вскрытия значений параметров защиты) m-й преграды u_m в комплексе должны быть таковыми, чтобы соответствующий расчетный риск не превышал допустимого. Из альтернативных вариантов предпочтение отдается тому варианту, для которого расчетный риск минимален при ограничениях на затраты и ресурсы.

Б.2.2.8 Условие по А.6.2, перечисление 8), по управлению безопасностью информации в части сохранения конфиденциальности используемой информации с помощью модели для оценки сохранения конфиденциальности используемой информации из ГОСТ Р 59341—2021, приложения В, В.3.9.3: для задаваемого периода объективной конфиденциальности используемой информации $T_{конф}$ количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы M, среднее время между соседними изменениями параметров защиты m-й преграды f_m и среднее время преодоления (вскрытия значений параметров защиты) m-й преграды u_m в комплексе должны быть таковыми, чтобы соответствующий расчетный риск не превышал допустимого.

Из альтернативных вариантов предпочтение отдается тому варианту, для которого расчетный риск минимален при ограничениях на затраты и ресурсы.

Б.2.3 Условия в части управления риском нарушения интероперабельности в моделируемой системе на техническом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемого условия α (применяются модель для оценки надежности предоставления информации (см. ГОСТ Р 59341—2021, приложение В, В.3.2), модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий (см. ГОСТ Р 59341—2021, приложение В, В.3.9.2; см. также А.6.3):

- частота возникновения источников угроз с точки зрения нарушения интероперабельности на техническом уровне σ не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы с точки зрения нарушения интероперабельности на техническом уровне β должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время системной диагностики целостности моделируемой системы $T_{диаг}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;
- среднее время восстановления нарушаемой целостности моделируемой системы $T_{восст}$ не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого.

Примечание — Необходимо учесть, что в реальности из определяемых в Б.2 условий с учетом специфики системы возможности управленческих воздействий на перечисленные характеристики могут быть практически ограничены; например, некоторые из средств, способов и действий, влияющих на выполнение условий могут оказаться технически не реализуемыми. Это означает, что в управлении контекстом использования системы эти условия игнорируются, применению подлежат лишь те условия, позволяющие удерживать риски в допустимых пределах, которые практически реализуемы.

Б.3 Для определения сбалансированных условий системной инженерии решению подлежат различные оптимизационные задачи. Например, постановка задачи может заключаться в определении таких условий использования моделируемой системы, для которых при задаваемых ограничениях достигается минимум интегрального риска нарушения интероперабельности в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов $R_{интегр}(T_{зад})$ с использованием формул (А.1)—(А.3).

При решении задач системной инженерии возможны другие постановки оптимизационных задач системного анализа, связанные, например, с максимизацией качества и/или безопасности и/или эффективности системы по показателям более высокого мета-уровня, когда расчетные значения интегрального риска нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов фигурируют в ограничениях, т. е. учитывается требование к допустимому значению интегрального риска: $R_{интегр}(T_{зад}) \le R_{доп}(T_{зад})$.

При этом могут быть использованы любые научно обоснованные формализованные модели и методы, обеспечивающие достижение целей и решение поставленных задач системной инженерии.

Типовые модели, методы и методики для определения существенных угроз и условий и решения прикладных задач системного анализа см. в приложении В.

Приложение В
(справочное)

Типовые модели, методы и методики для определения существенных угроз и условий и решения прикладных задач системного анализа

Для использования при решении различных прикладных задач системного анализа интероперабельности применительно к стандартизованным процессам ЖЦ различных систем в таблице В.1 приведены:

- ссылки на рекомендуемые типовые математические модели, методы, допустимые риски;
- примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа.

Примечание — Без ограничения общности в качестве дополнительных специфических требований, отраженных в наименованиях некоторых методик, использованы требования по защите информации.

Таблица В.1 — Типовые модели, методы и методики для определения существенных угроз и условий и решения прикладных задач системного анализа

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процессы приобретения и поставки продукции и услуг для системы	См. ГОСТ Р 59329—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59329—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса приобретения продукции и/или услуг для системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса приобретения продукции и/или услуг для системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса приобретения продукции и/или услуг для системы. Д.7 Методика прогнозирования риска нарушения требований по защите информации в процессе поставки продукции и/или услуг для системы. Д.8 Методика прогнозирования интегрального риска нарушения реализации процесса поставки продукции и/или услуг для системы с учетом требований по защите информации. Д.9 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.10 Методики выявления явных и скрытых недостатков процесса поставки продукции и/или услуг для системы с использованием прогнозирования рисков. Д.11 Методики обоснования предупреждающих действий, направленных на достижение целей процесса поставки продукции и/или услуг для системы и противодействие угрозам нарушения требований по защите информации. Д.12 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса поставки продукции и/или услуг для системы
Процесс управления моделью ЖЦ системы	См. ГОСТ Р 59330—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59330—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления моделью ЖЦ системы с использованием прогнозирования рисков.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс управления моделью ЖЦ системы	См. ГОСТ Р 59330—2021, методы, модели — приложение В; допустимые риски — приложение Г	Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления моделью ЖЦ системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления моделью ЖЦ системы
	См. ГОСТ Р 59992—2022, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59992—2022, перечень методик — приложение Д: Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности. Д.5 Методики определения существенных недостатков процесса управления моделью ЖЦ системы с использованием прогнозирования рисков. Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления моделью ЖЦ системы и противодействие угрозам. Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления моделью ЖЦ системы
Процесс управления инфраструктурой системы	См. ГОСТ Р 59331—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59331—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления инфраструктурой системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления инфраструктурой системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления инфраструктурой
	См. ГОСТ Р 59993—2022, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59993—2022, перечень методик — приложение Д: 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
Процесс управления портфелем проектов	См. ГОСТ Р 59332—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59332—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления портфелем проектов с использованием прогнозирования рисков.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс управления портфелем проектов	См. ГОСТ Р 59332—2021, методы, модели — приложение В; допустимые риски — приложение Г	Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления портфелем проектов и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления портфелем проектов
Процесс управления человеческими ресурсами системы	См. ГОСТ Р 59333—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59333—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления человеческими ресурсами системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления человеческими ресурсами системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления человеческими ресурсами
Процесс управления качеством системы	См. ГОСТ Р 59334—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59334—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления качеством системы с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления качеством системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления качеством системы
	См. ГОСТ Р 59989—2022, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59989—2022, перечень методик — приложение Д: Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности (в терминах обобщенного риска нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований). Д.5 Методики определения существенных недостатков процесса управления качеством системы с использованием прогнозирования рисков. Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления качеством системы и противодействие угрозам. Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления качеством системы
Процесс управления знаниями о системе	См. ГОСТ Р 59335—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59335—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс управления знаниями о системе	См. ГОСТ Р 59335—2021, методы, модели — приложение В; допустимые риски — приложение Д	Е.4 Методики выявления явных и скрытых недостатков процесса управления знаниями о системе с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления знаниями о системе и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления знаниями о системе
Процесс планирования проекта	См. ГОСТ Р 59336—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59336—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса планирования проекта с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса планирования проекта и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса планирования проекта
Процесс оценки и контроля проекта	См. ГОСТ Р 59337—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59337—2021, перечень методик — приложение Д
	См. ГОСТ Р 59990—2022, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59990—2022, перечень методик — приложение Д. Дополнительно к методикам, на которые сделаны ссылки в приложении Д, рекомендуется создание и применение методик, способствующих решению задач системной инженерии, в том числе: - методики оценки специальных показателей, связанных с критичными сущностями проекта и системы, охватываемой проектом; - методики обоснования допустимых значений специальных показателей, связанных с критичными сущностями проекта и системы, охватываемой проектом; - методики оценки интегрального риска нарушения качества, безопасности и эффективности системы, охватываемой проектом, в условиях возможных комбинаций, используемых системных процессов в задаваемом периоде прогноза; - методики определения существенных угроз и условий для проекта с использованием специальных показателей и прогнозируемых рисков; - комплекса методик поддержки принятия решений по обеспечению качества, безопасности и эффективности системы, охватываемой проектом, в ее ЖЦ; - методики обоснования упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства конкретных процесса, системы (и ее элементов) и проекта при задаваемых ограничениях (природных, технических, ресурсных, стоимостных, временных, социальных, экологических) в задаваемый период времени;

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс оценки и контроля проекта	См. ГОСТ Р 59990—2022, методы, модели — приложение В; допустимые риски — приложение Г	- методики обоснования предложений по обеспечению и повышению качества, безопасности и эффективности системы, охватываемой проектом (и ее элементов); - методики решения вспомогательных задач совершенствования непосредственно системного анализа процесса оценки и контроля проекта
Процесс управления решениями	См. ГОСТ Р 59338—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59338—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления решениями с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления решениями и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления решениями
Процесс управления рисками для системы	См. ГОСТ Р 59339—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59339—2021, перечень методик — приложение Е
	См. ГОСТ Р 59991—2022, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59991—2022, перечень методик — приложение Е. Дополнительно к методикам, на которые сделаны ссылки, рекомендуется создание и применение методик, способствующих решению задач системной инженерии, в том числе: - методики оценки специальных показателей, связанных с критичными сущностями системы; - методики обоснования допустимых значений специальных показателей, связанных с критичными сущностями системы; - методики оценки интегрального риска нарушения качества системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики оценки интегрального риска нарушения безопасности системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики оценки интегрального риска нарушения эффективности системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики определения существенных угроз и условий для конкретных процессов, системы и/или проекта с использованием специальных показателей и прогнозируемых рисков; - комплекса методик поддержки принятия решений по обеспечению качества, безопасности и эффективности системы в ее ЖЦ; - методики обоснования упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства конкретных процесса, системы (и ее элементов) и соответствующего проекта при задаваемых ограничениях (природных, технических, ресурсных, стоимостных, временных, социальных, экологических) в задаваемый период времени; - методики обоснования предложений по обеспечению и повышению качества, безопасности и эффективности системы (и ее элементов);

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс управления рисками для системы	См. ГОСТ Р 59991—2022, методы, модели — приложение В; допустимые риски — приложение Д	- методики решения вспомогательных задач совершенствования непосредственно системного анализа процесса управления рисками для системы
Процесс управления информацией системы	См. ГОСТ Р 59340—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59340—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления конфигурацией системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления конфигурацией системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления конфигурацией системы
	См. ГОСТ Р 59341—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59341—2021, перечень методик — приложение Е: Е.3 Методика количественного обоснования требований к системе и необходимых условий для обеспечения надежности предоставления информации. Е.4 Методика количественного обоснования требований к системе и необходимых условий для обеспечения своевременности предоставления информации. Е.5 Методика количественного обоснования требований к системе и необходимых условий для обеспечения полноты отражения состояния всех реально существующих критичных объектов и явлений. Е.6 Методика количественного обоснования требований к системе и необходимых условий для обеспечения актуальности информации на момент ее использования. Е.7 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности информации после ее контроля. Е.8 Методика количественного обоснования требований к системе и необходимых условий для получения корректных результатов обработки информации. Е.9 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности действий пользователей и персонала. Е.10 Методика количественного обоснования требований к системе и необходимых условий для обеспечения отсутствия опасного программно-технического воздействия на систему в пределах допустимого риска. Е.11 Методика количественного обоснования требований к системе для обеспечения защищенности активов системы от НСД в пределах допустимого риска. Е.12 Методика количественного обоснования требований к системе для сохранения конфиденциальности информации в пределах допустимого риска. Е.13 Методика прогнозирования интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс управления информацией системы	См. ГОСТ Р 59341—2021, методы, модели — приложение В; допустимые риски — приложение Д	Е.14 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации). Е.15 Методики выявления явных и скрытых недостатков процесса управления информацией системы с использованием прогнозирования рисков. Е.16 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления информацией системы и противодействие угрозам нарушения требований по защите информации (с использованием прогнозируемых рисков). Е.17 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления информацией системы (с использованием прогнозируемых рисков)
Процесс измерений системы	См. ГОСТ Р 59342—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59342—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса измерений системы с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса измерений системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса измерений системы
Процесс гарантии качества для системы	См. ГОСТ Р 59343—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59343—2021, перечень методик — приложение Е
	См. ГОСТ Р 59994—2022, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59994—2022, перечень методик — приложение Д
Процесс анализа бизнеса или назначения системы	См. ГОСТ Р 59344—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59344—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса анализа бизнеса или назначения системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса анализа бизнеса или назначения системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса анализа бизнеса или назначения системы

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс определения потребностей и требований заинтересованной стороны для системы	См. ГОСТ Р 59345—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59345—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса определения потребностей и требований заинтересованной стороны для системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса определения потребностей и требований заинтересованной стороны для системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения потребностей и требований заинтересованной стороны для системы
Процесс определения системных требований	См. ГОСТ Р 59346—2021, методы, модели — приложения В, Д; допустимые риски — приложение Е	См. ГОСТ Р 59346—2021, методические указания — приложение Ж
Процесс определения архитектуры системы	См. ГОСТ Р 59347—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59347—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса определения архитектуры системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса определения архитектуры системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения архитектуры системы
Процесс определения проекта	См. ГОСТ Р 59348—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59348—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса определения проекта с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса определения проекта и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения проекта
Процесс системного анализа	См. ГОСТ Р 59349—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59349—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс системного анализа	См. ГОСТ Р 59349—2021, методы, модели — приложение В; допустимые риски — приложение Д	Е.4 Методики выявления явных и скрытых недостатков процесса системного анализа с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер для достижения целей процесса системного анализа и противодействия угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам исследований процесса системного анализа. Е.7 Методики выявления явных и скрытых угроз нарушения надежности реализации системных процессов (по ГОСТ Р 57193) с использованием прогнозирования рисков. Е.8 Методики решения задач минимизации интегрального риска нарушения безопасности системы при кратко-, средне- и долгосрочном планировании и ограничениях (на отдельные допустимые риски реализации существенных угроз, на ресурсы, общие затраты и при иных ограничениях), учитывающих специфику системы. Е.9 Методики решения задач минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях (на интегральный риск нарушения безопасности системы, на отдельные допустимые риски реализации существенных угроз, на ресурсы и при иных ограничениях), учитывающих специфику системы
Процесс реализации системы	См. ГОСТ Р 59350—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59350—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса реализации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса реализации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса реализации системы
Процесс комплексирования системы	См. ГОСТ Р 59351—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59351—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса комплексирования системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса комплексирования системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса комплексирования системы
Процесс верификации системы	См. ГОСТ Р 59352—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59352—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации.

Продолжение таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс верификации системы	См. ГОСТ Р 59352—2021, методы, модели — приложение В; допустимые риски — приложение Г	Д.4 Методики выявления явных и скрытых недостатков процесса верификации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса верификации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса верификации системы
Процесс передачи системы	См. ГОСТ Р 59353–2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59353—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса передачи системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса передачи системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса передачи системы
Процесс аттестации системы	См. ГОСТ Р 59354—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59354—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса аттестации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса аттестации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам аттестации системы
Процесс функционирования системы	См. ГОСТ Р 59355—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59355—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации). Е.4 Методики выявления явных и скрытых недостатков процесса функционирования системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса функционирования системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам функционирования системы. Е.7 Методики инструментально-расчетной оценки показателей устойчивости функционирования системы в условиях информационно-технических воздействий.

Окончание таблицы В.1

Системные процессы	Ссылки на типовые модели, методы, допустимые риски	Примерный перечень методик для определения существенных угроз и условий и решения прикладных задач системного анализа
Процесс функционирования системы	См. ГОСТ Р 59355—2021, методы, модели — приложение В; допустимые риски — приложение Д	Е.8 Методики обоснования способов повышения устойчивости функционирования системы в условиях информационно-технических воздействий
Процесс сопровождения системы	См. ГОСТ Р 59356—2021, методы, модели — приложение В; допустимые риски — приложение Д	См. ГОСТ Р 59356—2021, перечень методик — приложение Е: Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса сопровождения системы с использованием прогнозируемых рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса сопровождения системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса сопровождения системы
Процесс изъятия и списания системы	См. ГОСТ Р 59357—2021, методы, модели — приложение В; допустимые риски — приложение Г	См. ГОСТ Р 59357—2021, перечень методик — приложение Д: Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса изъятия и списания системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса изъятия и списания системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса изъятия и списания системы

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 10 января 2002 г. № 7-ФЗ «Об охране окружающей среды»

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

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

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

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

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

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

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

[12] Постановление Правительства Российской Федерации от 12 февраля 2021 г. № 171 «О Координационном центре Правительства Российской Федерации»

УДК 006.34:004.056:006.354 ОКС 35.080

Ключевые слова: системная инженерия, безопасность, интероперабельность, системный анализ, качество, модель, показатель, риск, система, угроза, условие, характеристика

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 13.01.2026. Подписано в печать 12.02.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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