ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59339— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ РИСКАМИ ДЛЯ СИСТЕМЫ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФГУ ФИЦ ИУ РАН), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ ГНИИИ ПТЗИ ФСТЭК России), Федеральным бюджетным учреждением «Научно-технический центр «Энергобезопасность» (ФБУ «НТЦ Энергобезопасность») и Обществом с ограниченной ответственностью «Научно-исследовательский институт прикладной математики и сертификации» (ООО НИИПМС)

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 апреля 2021 г. № 330-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе управления рисками для системы 7
5 Общие требования системной инженерии по защите информации в процессе управления рисками для системы 8
6 Специальные требования к количественным показателям 10
7 Требования к системному анализу 13
Приложение А (справочное) Пример перечня защищаемых активов 14
Приложение Б (справочное) Пример перечня угроз 15
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 16
Приложение Г (справочное) Методические указания по прогнозированию рисков 22
Приложение Д (справочное) Рекомендации по определению допустимых значений показателей рисков 38
Приложение Е (справочное) Рекомендации по перечню методик системного анализа 40
Библиография 41

Введение

Настоящий стандарт расширяет комплекс национальных стандартов системной инженерии по защите информации при планировании и реализации процессов в жизненном цикле различных систем. Выбор и применение реализуемых процессов для системы в ее жизненном цикле осуществляют по ГОСТ Р 57193. Методы системной инженерии в интересах защиты информации применяют для системных процессов:

- процессов соглашения — процессов приобретения и поставки продукции и услуг для системы — по ГОСТ Р 59329;

- процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;

- процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, конфигурацией, информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343. В приложении к процессу управления рисками для системы — по настоящему стандарту;

- технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы — по 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.

Стандарт устанавливает основные требования системной инженерии по защите информации в процессе управления рисками для системы и специальные требования к используемым количественным показателям. Для планируемого и реализуемого процесса управления рисками применение настоящего стандарта при создании (модернизации, развитии), эксплуатации систем и выведении их из эксплуатации обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ РИСКАМИ ДЛЯ СИСТЕМЫ

System engineering. Protection of information in risk management process for system

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа для процесса управления рисками для системы применительно к вопросам защиты информации в системах различных областей приложения.

Для практического применения в приложениях А—Е приведены примеры перечней активов, подлежащих защите, и угроз, типовые методы, модели и методические указания по прогнозированию рисков, рекомендации по определению допустимых значений для показателей рисков, а также рекомендации по перечню методик системного анализа.

Примечание — Оценка ущербов выходит за рамки настоящего стандарта. Для разработки самостоятельной методики по оценке ущербов учитывают специфику систем (см., например, ГОСТ Р 22.10.01, ГОСТ Р 54145). При этом должны учитываться соответствующие положения законодательства Российской Федерации.

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процесс управления рисками для системы, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем — см. примеры систем в [1]—[26].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

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

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

Издание официальное

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

ГОСТ Р ИСО 14258 Промышленные автоматизированные системы. Концепции и правила для моделей предприятия

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

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

ГОСТ Р ИСО 15704 Промышленные автоматизированные системы. Требования к стандартным архитектурам и методологиям предприятия

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

ГОСТ Р 51904 Программное обеспечение встроенных систем. Общие требования к разработке и документированию

ГОСТ Р 53647.1 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

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

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

ГОСТ Р 57100/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры

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

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

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 59329—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 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 МЭК 61069-1 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 1. Терминология и общие концепции

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р МЭК 62508 Менеджмент риска. Анализ влияния на надежность человеческого фактора

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

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 34.003, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, 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 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, а также следующие термины с соответствующими определениями:

3.1.1

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.2

заинтересованная сторона, правообладатель: Индивидуум или организация, имеющие право, долю, требование или интерес в системе или в обладании ее характеристиками, удовлетворяющими их потребности и ожидания.

Пример — Конечные пользователи, организации конечного пользователя, поддерживающие стороны, разработчики, производители, обучающие стороны, сопровождающие и утилизирующие организации, приобретающие стороны, организации поставщика, органы регуляторов.

Примечание — Некоторые заинтересованные стороны могут иметь противоположные интересы в системе.

[ГОСТ Р 57193—2016, пункт 4.1.42]

3.1.3

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]

3.1.4

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]

3.1.5

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]

3.1.6

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]

3.1.7 **интегральный риск нарушения реализации процесса управления рисками для системы с учетом требований по защите информации:** Сочетание вероятности того, что будут нарушены надежность реализации процесса управления рисками для системы либо требования по защите информации, либо и то, и другое, с тяжестью возможного ущерба.

3.1.8 **моделируемая система:** Система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения.

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

3.1.9 **надежность реализации процесса:** Свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить его в заданных условиях реализации.

3.1.10

норма эффективности защиты информации: Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.11

показатель эффективности защиты информации: Мера или характеристика для оценки эффективности защиты информации.

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.12

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.13 **система-эталон:** Реальная или гипотетичная система, которая по своим показателям интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации принимается в качестве эталона для полного удовлетворения требований заинтересованных сторон системы и рационального решения задач системного анализа, связанных с обоснованием допустимых рисков, обеспечением нормы эффективности защиты информации, обоснованием мер, направленных на достижение целей процесса, противодействие угрозам и определение сбалансированных решений при средне- и долгосрочном планировании, а также с обоснованием предложений по совершенствованию и развитию системы защиты информации.

3.1.14

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.1.15 **скрытые угрозы системе:** Неявные угрозы, выявление которых осуществляют лишь по признакам, косвенно связанным с возможными реальными угрозами, а распознавание — путем оценки развития предпосылок к нарушению нормальных условий существования и/или функционирования системы.

3.1.16

требование по защите информации: Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

[ГОСТ Р 50922—2006, статья 2.9.2]

3.1.17

угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

[ГОСТ Р 50922—2006, статья 2.6.1]

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

3.1.19

эффективность защиты информации: Степень соответствия результатов защиты информации цели защиты информации.

[ГОСТ Р 50922—2006, статья 2.9.1]

3.1.20 **явные угрозы системе:** Угрозы нормальным условиям существования и/или функционирования системы, однозначное выявление и распознавание которых возможно по заранее определенным и реально проявляемым свойственным признакам.

3.2 В настоящем стандарте использовано сокращение:

ТЗ — техническое задание.

4 Основные положения системной инженерии по защите информации в процессе управления рисками для системы

4.1 Общие положения

Организации используют данный процесс в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения ее качества, безопасности и эффективности, а также при выведении системы из эксплуатации для обеспечения требований безопасности.

В процессе управления рисками для системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

Для прогнозирования рисков, связанных с реализацией процесса, и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах используют системный анализ процесса с учетом требований по защите информации.

Определение выходных результатов процесса управления рисками для системы и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51904, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Определение интегральных рисков в системных процессах с учетом требований по защите информации осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59355. При этом учитывают специфику организации, применяющей процесс, и специфику самой системы (см., например, [21]—[26]).

4.2 Стадии и этапы жизненного цикла системы

Процесс управления рисками используют на любой стадии жизненного цикла системы. Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации системы устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839. Процесс управления рисками для системы входит в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости может включать в себя другие процессы.

4.3 Цели процесса и назначение мер защиты информации

4.3.1 Определение целей процесса управления рисками для системы осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508 с учетом специфики системы.

В общем случае главная цель процесса управления рисками для системы состоит в своевременной идентификации рисков, обосновании и реализации эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

4.3.2 Меры защиты информации в процессе управления рисками для системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер по защите информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [20]—[24] с учетом специфики системы и реализуемой стадии жизненного цикла.

4.4 Основные принципы

При проведении системного анализа процесса управления рисками для системы руководствуются основными принципами, определенными в ГОСТ Р 59349 с учетом дифференциации требований по защите информации в зависимости от категории значимости системы и важности обрабатываемой в ней информации — см. ГОСТ Р 59346, [19]—[24]. Все применяемые принципы подчинены принципу целенаправленности осуществляемых действий.

4.5 Основные усилия системной инженерии

Основные усилия системной инженерии для обеспечения защиты информации в процессе управления рисками для системы сосредотачивают:

- на определении выходных результатов и действий, предназначенных для достижения целей процесса и защиты активов, информация которых или о которых необходима для достижения этих целей;
- выявлении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для активов, подлежащих защите, выходных результатов и выполняемых действий процесса;
- определении и прогнозировании рисков, подлежащих системному анализу;
- проведении системного анализа для обоснования мер, направленных на противодействие угрозам и достижение целей процесса.

5 Общие требования системной инженерии по защите информации в процессе управления рисками для системы

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы, в качестве каковой может выступать система защиты информации, в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований формируют при выполнении процесса

определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например, [1]—[26]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

Поскольку элементы процесса управления рисками для системы могут использоваться на этапах, предваряющих получение и утверждение ТЗ, соответствующие требования по защите информации, применимые к этому процессу, могут быть оговорены в рамках соответствующих договоров и соглашений.

Примечание — Если информация относится к категории государственной тайны, в вопросах защиты информации руководствуются регламентирующими документами соответствующих государственных регуляторов. При использовании процесса управления рисками для систем искусственного интеллекта необходимо гарантированно подтверждать достаточность автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации), учитывать возможность повышения уровня конфиденциальности данных в процессе их обработки в системе искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации), регламентировать вопросы обеспечения конфиденциальности тестовых выборок исходных данных, используемых испытательными лабораториями при оценке соответствия прикладных систем искусственного интеллекта, с сохранением прозрачности и подотчетности этого процесса.

5.2 Требования системной инженерии по защите информации призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации процесса управления рисками для системы и поддержке при этом эффективности защиты информации.

Требования системной инженерии по защите информации в процессе управления рисками для системы включают:

- требования к определению заинтересованных сторон, имеющих интерес к рассматриваемой системе, выходных результатов процесса, выполняемых действий и используемых при этом активов, требующих защиты информации;

- требования к определению потенциальных угроз для выходных результатов и выполняемых действий процесса, а также возможных сценариев возникновения и развития этих угроз;

- требования к прогнозированию рисков при планировании и реализации системных процессов, обоснованию эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

5.3 Состав выходных результатов и выполняемых действий в процессе управления рисками для системы определяют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики системы.

5.4 Меры защиты информации и действия по защите информации должны охватывать активы, информация которых или о которых необходима для получения выходных результатов и выполнения действий в процессе управления рисками для системы.

Примечание — В состав активов могут быть включены активы, используемые для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика — например, привлекаемые информационные системы и/или базы данных поставщиков.

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом рекомендаций ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6 и специфики системы (см., например, [21]—[26]).

Примеры перечней учитываемых активов и угроз в процессе управления рисками для системы приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процесса управления рисками анализируют по показателям рисков в зависимости от специфики системы, целей ее применения и возможных угроз при выполнении процесса. В системном анализе процесса используют модель угроз безопасности информации.

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508, [21]—[26].

5.7 Для обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах применяют системный анализ с использованием устанавливаемых специальных качественных и количественных показателей рисков. Качественные показатели для оценки рисков в области информационной безопасности определены в ГОСТ Р ИСО/МЭК 27005. Целесообразность использования количественных показателей рисков в дополнение к качественным показателям может потребовать дополнительного обоснования. Состав специальных количественных показателей рисков в интересах системного анализа определен в 6.3.

Типовые модели и методы процесса управления рисками для системы, методические указания по прогнозированию рисков, рекомендации по допустимым значениям показателей рисков и по перечню методик системного анализа приведены в приложениях В, Г, Д, Е. Характеристики мер и действий по защите информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам, исходя из возможных условий их реализации.

6 Специальные требования к количественным показателям

6.1 Общие положения

6.1.1 В приложении к защищаемым активам, действиям и выходным результатам процесса управления рисками для системы, к которым предъявлены определенные требования по защите информации, выполняют оценку эффективности защиты информации на основе прогнозирования рисков в условиях возможных угроз.

6.1.2 В общем случае основными выходными результатами процесса управления рисками для системы являются.

- результаты идентификации рисков;
- результаты прогнозирования, оценки и анализа рисков;
- возможные варианты реакции на риски и их приоритетность;
- результаты обоснования предупреждающих мер по снижению рисков или их удержанию в допустимых пределах;
- достигаемые эффекты от реализации предупреждающих мер реакции на риски;
- результаты анализа изменений в функционировании, совершенствовании и развитии системы в условиях реакции на риски.

6.1.3 Для получения выходных результатов процесса управления рисками в общем случае выполняют следующие основные действия:

- планирование и управление профилем рисков, включая:
  - определение стратегии управления рисками для всех иерархических уровней системы, в том числе в цепочке поставок продукции и/или услуг для системы,
  - определение и документирование контекста процесса управления рисками для системы (в том числе описание требований заинтересованных сторон, технических и управленческих целей), формирование предположений и ограничений, определение множества возможных событий, способных привести к рисковым ситуациям, улучшению, предотвращению, ухудшению, ускорению или задержкам в достижении целей системы (в том числе рассмотрение рисков, связанных с недоиспользованием возможностей и недостижением эффектов от реализации возможностей),
  - определение, обоснование и документирование допустимых рисков и условий, при которых риски могут быть приняты на допустимом уровне,
  - определение и сопровождение профиля рисков, ведение отчетности о состоянии каждого из рисков (в том числе определение частоты возникновения угроз, времени их развития, периодичности и длительности контроля целостности отслеживаемых параметров, времени восстановления целостности после нарушений, определение возможных последствий и

допустимых уровней рисков), весомость каждого риска, возможные действия, планируемые в качестве реакции на недопустимые риски, включая определение необходимых ресурсов,

- доведение профиля рисков до заинтересованных сторон согласно их потребностям;

- прогнозирование, оценку и анализ рисков, включая:
  - идентификацию рисков в категориях, описанных в контексте управления рисками, в том числе через различные исследования надежности, безопасности, производительности, качества и эффективности системы, оценки технологий и архитектуры, анализ альтернативных решений,
  - прогнозирование рисков, оценку вероятности реализации угроз и возможного ущерба по каждому из идентифицированных рисков, оценивание рисков в сравнении с допустимым уровнем,
  - для каждого риска, превышающего допустимый уровень, — определение, обоснование и документирование рекомендуемых упреждающих мер противодействия угрозам (направленных на уменьшение риска или смягчение возможных негативных последствий);
- реагирование на риски:
  - выбор альтернативных решений для реакции на риски (в том числе упреждающих мер противодействия угрозам),
  - реализацию мер реакции для снижения рисков до допустимого уровня и удержания рисков в допустимых пределах,
  - осуществление мониторинга критичных параметров и количественного прогнозирования и анализа рисков в случаях, когда повышенный риск (превышающий установленный допустимый уровень) принимается заинтересованными сторонами для определения необходимости каких-либо дополнительных возможных действий по реагированию на это превышение,
  - целенаправленное применение упреждающих мер реакции на риски;
- непрерывный контроль рисков, включая:
  - контроль идентифицированных рисков и контекста управления рисками во времени (для прогнозирования и оценки рисков в динамике их изменений);
  - количественный анализ показателей рисков, включая сравнение с прогнозируемыми ранее рисками (для оценки эффективности принятых ранее и дополнительных упреждающих мер, а также оценки реакции на риски);
  - выявление новых рисков и источников угроз в различных процессах, планируемых и реализуемых в жизненном цикле системы.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процесса, являются основой для принятия решений по факту наступления событий и источником исходных данных для прогнозирования рисков на задаваемый период прогноза. Риски оценивают вероятностными показателями с учетом возможного ущерба (см. приложения В, Г).

6.2 Требования к составу показателей

Выбираемые показатели должны обеспечивать проведение оценки эффективности защиты информации, прогнозирование и управление рисками для системы с учетом требований по защите информации.

Эффективность защиты информации оценивают с помощью количественных показателей, которые позволяют сформировать представление о текущих и потенциальных проблемах или о возможных причинах недопустимого снижения эффективности на ранних этапах проявления явных и скрытых угроз безопасности информации, когда можно принять предупреждающие меры. Дополнительно могут быть использованы вспомогательные статистические показатели, характеризующие события, которые уже произошли, и их влияние на эффективность защиты информации при реализации различных процессов в жизненном цикле системы. Вспомогательные показатели позволяют исследовать произошедшие события и их последствия и сравнивать эффективность применяемых и/или возможных мер в действующей системе защиты информации.

6.3 Требования к количественным показателям

6.3.1 Для прогнозирования рисков используют:

- для каждого из рассматриваемых процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления и технических процессов (за исключением процесса определения системных требований):

- риск нарушения надежности реализации процесса без учета требований по защите информации,
- риск нарушения требований по защите информации в процессе,
- интегральный риск нарушения реализации процесса с учетом требований по защите информации;

- для рассматриваемого технического процесса определения системных требований по ГОСТ Р 59346:
  - частные показатели риска реализации угроз безопасности информации в условиях отсутствия мер защиты информации, предлагаемых к применению в ходе формирования системных требований,
  - частные показатели риска реализации угроз безопасности информации в случае применения мер защиты информации, предлагаемых в ходе формирования системных требований (показатели остаточного риска при нарушении требований по защите информации),
  - интегральный риск нарушения функционирования системы и утечки защищаемой информации при применении мер защиты информации, предлагаемых в ходе формирования системных требований,
  - показатель риска нарушения надежности процесса обоснования системных требований в части защиты информации.

6.3.2 Риски нарушения надежности реализации конкретного процесса без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности его реализации (без учета требований по защите информации) в сопоставлении с возможным ущербом.

6.3.3 Риски нарушения требований по защите информации в конкретном процессе характеризуют соответствующей вероятностью нарушения требований по защите информации в сопоставлении с возможным ущербом. При расчетах должны быть учтены защищаемые активы, действия рассматриваемого процесса и выходные результаты, к которым предъявляются определенные требования по защите информации.

6.3.4 Интегральный риск нарушения реализации конкретного процесса с учетом требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса (без учета требований по защите информации) и вероятностью нарушения требований по защите информации в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

- временные данные функционирования системы защиты информации, в том числе срабатывания ее исполнительных механизмов;
- текущие и статистические данные о состоянии параметров системы защиты информации (привязанные к временам изменения состояний);
- текущие и статистические данные о самой системе или системах-аналогах, характеризующие не только данные о нарушениях надежности реализации процесса, но и события, связанные с утечкой защищаемой информации, несанкционированными или непреднамеренными воздействиями на защищаемую информацию (привязанные к временам наступления событий, характеризующих нарушения и предпосылки к нарушениям требований по защите информации);
- текущие и статистические данные результатов технического диагностирования системы защиты информации;
- наличие и готовность персонала системы защиты информации, данные об ошибках персонала (привязанные к временам наступления событий, последовавших из-за этих ошибок и характеризующих нарушения и предпосылки к нарушениям требований по защите информации) в самой системе или в системах-аналогах;
- данные из модели угроз безопасности информации и метаданные, позволяющие сформировать перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для каждого из защищаемых активов.

Типовые исходные данные для моделирования указаны в ссылках на рекомендуемые методы и модели в приложении В.

7 Требования к системному анализу

Требования к системному анализу в процессе управления рисками для системы включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в жизненном цикле рассматриваемой системы.

Общие применимые рекомендации для проведения системного анализа изложены в ГОСТ Р 59349.

При обосновании и формулировании требований к системному анализу дополнительно руководствуются положениями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы (см., например, [21]—[26]).

Примечание — Примеры решения задач системного анализа в приложении к различным процессам и системам — см. ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе управления рисками для системы может включать (в части, свойственной этому процессу):

- выходные результаты процесса — по 6.1.2;
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации — см., например, [21]—[24];
- договоры и соглашения на проведение работ по созданию (модернизации, развитию) системы или по выведению системы из эксплуатации;
- лицензии, подтверждающие право поставщика (производителя) на проведение работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- финансовые и плановые документы, связанные с эксплуатацией системы, проведением работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- документацию при выполнении научно-исследовательских работ (по ГОСТ 7.32, ГОСТ 15.101) с учетом специфики системы;
- конструкторскую и технологическую документацию (для модернизируемой или применяемой системы) — по ГОСТ 3.1001, ГОСТ 34.201;
- эксплуатационную и ремонтную документацию — по ГОСТ 2.602, ГОСТ 34.201, ГОСТ Р 2.601 с учетом специфики системы;
- документацию системы менеджмента качества организации — по ГОСТ Р ИСО 9001;
- технические задания — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839 с учетом специфики системы;
- персональные данные, базу данных и базу знаний, систему хранения архивов;
- систему передачи данных и облачные данные организации;
- выходные результаты иных процессов в жизненном цикле системы с учетом ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе управления рисками для системы может включать (в части, свойственной этому процессу):

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275;
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124;
- угрозы безопасности информации при подготовке и обработке документов — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412;
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному приобретателю (заказчику), информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги;
- прочие соответствующие угрозы безопасности информации, связанные с управлением рисками, для информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов из Банка данных угроз, сопровождаемого государственным регулятором.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

Процесс управления рисками для системы применим ко всем системным процессам (процессам соглашения, процессам организационного обеспечения проекта, процессам технического управления, техническим процессам), в том числе непосредственно к себе самому. В настоящем приложении приведены ссылки на стандарты системной инженерии, содержащие рекомендации по типовым моделям и методам прогнозирования рисков во всех системных процессах, — см. таблицу В.1. Эти методы и модели в полной мере применимы в процессе управления рисками для системы.

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

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процессы приобретения и поставки продукции и услуг для системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59329—2021, приложение В
Процесс управления моделью жизненного цикла системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59330—2021, приложение В
Процесс управления инфраструктурой системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59331—2021, приложение В
Процесс управления портфелем проектов	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59332—2021, приложение В
Процесс управления человеческими ресурсами системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе;	ГОСТ Р 59333—2021, приложение В

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс управления человеческими ресурсами системы	в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59333—2021, приложение В
Процесс управления качеством системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59334—2021, приложение В
Процесс управления знаниями о системе	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59335—2021, приложение В
Процесс планирования проекта	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59336—2021, приложение В
Процесс оценки и контроля проекта	По ГОСТ Р 59337—2021, подраздел 6.3	ГОСТ Р 59337—2021, приложение В
Процесс управления решениями	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59338—2021, приложение В
Процесс управления рисками для системы	По 6.3	Настоящий стандарт, приложение В
Процесс управления конфигурацией системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59340—2021, приложение В

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс управления информацией системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59341—2021, приложение В
Процесс измерений системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59342—2021, приложение В
Процесс гарантии качества для системы	По ГОСТ Р 59343—2021, подраздел 6.3	ГОСТ Р 59343—2021, приложение В
Процесс анализа бизнеса или назначения системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59344—2021, приложение В
Процесс определения потребностей и требований заинтересованной стороны для системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59345—2021, приложение В
Процесс определения системных требований	а) частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения функционирования системы); б) частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения требований по защите конфиденциальной информации в системе или о системе);	ГОСТ Р 59346—2021, приложения В, Д

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс определения системных требований	в) интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований	ГОСТ Р 59346—2021, приложения В, Д
Процесс определения архитектуры системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59347—2021, приложение В
Процесс определения проекта	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59348—2021, приложение В
Процесс системного анализа	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59349—2021, приложение В
Процесс реализации системы	а) риск нарушения надежности выполнения процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения выполнения процесса с учетом требований по защите информации	ГОСТ Р 59350—2021, приложение В
Процесс комплексирования системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59351—2021, приложение В

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс верификации системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59352—2021, приложение В
Процесс передачи системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59353—2021, приложение В
Процесс аттестации системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59354—2021, приложение В
Процесс функционирования системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59355—2021, приложение В
Процесс сопровождения системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59356—2021, приложение В
Процесс изъятия и списания системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе;	ГОСТ Р 59357—2021, приложение В

Окончание таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс изъятия и списания системы	в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59357—2021, приложение В

Примечание — Другие возможные показатели, модели и методы оценки 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 58494, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков

Г.1 Общие положения

Настоящие методические указания определяют типовые действия в процессе управления рисками для системы. При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможными оценками ущербов.

Расчетные значения рисков на заданный период прогноза используют для решения задач системного анализа при выполнении работ системной инженерии. Синергетические эффекты системной инженерии достигаются за счет количественно обоснованного целенаправленного уменьшения различных рисков или удержания рисков в допустимых пределах при реализации каждого из процессов соглашения, организационного обеспечения проекта, технического управления и технических процессов на всех этапах жизненного цикла систем — 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 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.

Примечание — Дополнительно могут быть востребованы методики по оценке ущербов, учитывающие специфику системы (см., например, ГОСТ Р 22.10.01, ГОСТ Р 54145).

Г.2 Анализируемые объекты для прогнозирования рисков

Применительно к конкретной системе для прогнозирования рисков нарушения требований по защите информации в процессе управления рисками для системы согласно 5.2, 5.3, 6.1 настоящего стандарта определению подлежат:

- состав заинтересованных сторон, имеющих интерес к рассматриваемой системе;
- состав выходных результатов и выполняемых действий процесса управления рисками для системы и используемых при этом активов;
- перечень потенциальных угроз и возможных сценариев возникновения и развития угроз для выходных результатов и выполняемых действий процесса управления рисками для системы;
- иные объекты, используемые в прогнозировании рисков при необходимости оценки того, насколько организация процесса управления рисками способна обеспечить возможности по его выполнению в заданной среде применения системы.

Г.3 Цель прогнозирования рисков

Основной целью прогнозирования рисков является установление степени вероятного нарушения требований по защите информации и/или нарушения надежности реализации исследуемых системных процессов (процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления, технических процессов) с учетом требований по защите информации за заданный период прогноза. Прогнозирование рисков осуществляют в интересах решения определенных задач системного анализа при планировании и реализации системных процессов, обосновании эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах. Конкретные практические цели прогнозирования рисков устанавливают заказчик системного анализа и/или аналитик моделируемой системы при выполнении работ системной инженерии.

Г.4 Используемые методы и модели

Для выполнения необходимых работ системной инженерии, связанных с прогнозированием рисков, используют методы и модели (см. приложение В), устанавливают ограничения на допустимые риски (см. приложение Д), разрабатывают необходимые методики системного анализа (см. приложение Е).

Г.5 Порядок прогнозирования рисков

Г.5.1 Для прогнозирования рисков осуществляют следующие шаги.

Шаг 1. Определяют моделируемые системы и устанавливают анализируемые объекты для прогнозирования рисков — действия осуществляют согласно Г.1.

Шаг 2. Устанавливают конкретные цели прогнозирования — действия осуществляют согласно Г.2

Шаг 3. Формируют перечень возможных угроз. Принимают решение о представлении каждой из моделируемых систем в виде «черного ящика» или в виде сложной структуры, декомпозируемой до составных элементов. Формируют пространство элементарных состояний для каждого элемента и каждой моделируемой системы в целом — все действия осуществляют согласно Г.3.

Шаг 4. Согласно Г.4 выбирают расчетные показатели и подходящие математические модели и методы, приведенные в приложении В. Определяют допустимые риски — см. приложение Д. Разрабатывают необходимые методики системного анализа — см. приложение Е. Применительно к моделируемым системам формируют исходные

данные, необходимые для проведения расчетов. Осуществляют расчет выбранных показателей по выбранным и разработанным методам, моделям, методикам.

Г.5.2 Получаемые в результате моделирования значения рисков используют для решения задач системного анализа (см. раздел 7 и приложение Е).

Г.6 Обработка и использование результатов прогнозирования для управления рисками

Результаты прогнозирования рисков должны быть удобны для обработки заказчиком функционирования системы и/или аналитиком моделируемой системы. Результаты представляются в виде гистограмм, графиков, таблиц и/или в ином виде, позволяющем анализировать зависимости рисков от изменения значений исходных данных при решении задач системного анализа (см. раздел 7 и приложение Е). Результаты расчетов подлежат использованию для управления рисками при выполнении работ системной инженерии.

Возможные способы уменьшения рисков, которые могут быть количественно обоснованы с применением рекомендуемых методов и моделей, представляют собой механизмы непосредственно управления рисками при реализации каждого из системных процессов (процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления, технических процессов) — см. таблицу Г.1.

Таблица Г.1 — Возможные способы уменьшения рисков в результате управления

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процессы приобретения и поставки продукции и услуг для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса приобретения или поставки продукции и услуг для системы; соблюдение сроков поставки продукции и/или услуг; соблюдение уровня допустимого брака в поставляемых продукции и/или услугах
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе приобретения и поставки продукции и услуг для системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе приобретения и поставки продукции и услуг для системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процессов приобретения и поставки продукции и услуг для системы и защите информации в этих процессах, направленные на удержание рисков в допустимых пределах
Процесс управления моделью жизненного цикла системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса управления моделью жизненного цикла системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления моделью жизненного цикла системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления моделью жизненного цикла системы

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс управления моделью жизненного цикла системы	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления моделью жизненного цикла системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления инфраструктурой системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз нарушения надежности реализации процесса управления инфраструктурой системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления инфраструктурой системы
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления инфраструктурой системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления инфраструктурой системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления инфраструктурой системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления портфелем проектов	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса управления портфелем проектов; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления портфелем проектов (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления портфелем проектов
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления портфелем проектов и защите информации в процессе, направленные на удержание рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс управления человеческими ресурсами системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз нарушения надежности реализации процесса управления человеческими ресурсами системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления человеческими ресурсами системы
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления человеческими ресурсами системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления человеческими ресурсами системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления человеческими ресурсами системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления качеством системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса управления качеством системы; соблюдение сроков поставки продукции и/или услуг; соблюдение уровня допустимого брака в поставляемых продукции и/или услугах
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления качеством системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления качеством системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления качеством системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс управления знаниями о системе	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса приобретения знаний; соблюдение сроков поставки приобретаемых знаний; соблюдение уровня допустимого брака в приобретаемых знаниях; выполнение необходимых условий с завершением всех предпринимаемых действий процесса создания полезных знаний; соблюдение сроков создания полезных знаний; соблюдение уровня допустимого брака в создаваемых знаниях
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления знаниями о системе (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления знаниями о системе
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления знаниями о системе и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс планирования проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса планирования проекта; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе планирования проекта (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе планирования проекта
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса планирования проекта и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс оценки и контроля проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса оценки и контроля проекта; соблюдение сроков выполнения необходимых действий процесса

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В 1
Процесс оценки и контроля проекта	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе оценки и контроля проекта (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе оценки и контроля проекта
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса оценки и контроля проекта и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления решениями	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз нарушения надежности реализации процесса управления решениями (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления решениями
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления решениями (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления решениями
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления решениями и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления рисками для системы	По настоящему стандарту	По всем системным процессам — способы уменьшения рисков согласно приведенным в настоящей таблице
Процесс управления конфигурацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса управления конфигурацией системы; соблюдение сроков выполнения необходимых действий процесса

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс управления конфигурацией системы	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления конфигурацией системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления конфигурацией системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления конфигурацией системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс управления информацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обеспечение необходимой надежности представления используемой информации; обеспечение необходимой своевременности представления используемой информации; обеспечение необходимой полноты оперативного отражения в системе новых объектов и явлений; обеспечение необходимой актуальности обновляемой информации; обеспечение необходимой безошибочности информации после контроля; обеспечение необходимой корректности обработки информации; обеспечение необходимой безошибочности действий должностных лиц
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе управления информацией системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления информацией системы; сохранение целостности системы в условиях опасных программно-технических воздействий; обеспечение защищенности активов от несанкционированного доступа; сохранение конфиденциальности используемой информации
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса управления информацией системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс измерений системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса измерений системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе измерений системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе измерений системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса измерений системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс гарантии качества для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса гарантии качества для системы; повышение уверенности в ожидаемой готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе гарантии качества для системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе гарантии качества для системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса гарантии качества для системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс анализа бизнеса или назначения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса анализа бизнеса или назначения системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе анализа бизнеса или назначения системы (если это возможно при управлении рисками);

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс анализа бизнеса или назначения системы	Риск нарушения требований по защите информации в процессе	увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе анализа бизнеса или назначения системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса анализа бизнеса или назначения системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс определения потребностей и требований заинтересованной стороны для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса анализа бизнеса или назначения системы; повышение готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения потребностей и требований заинтересованной стороны для системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс определения системных требований	Частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения функционирования системы)	Защита системы от вредоносного программного обеспечения; межсетевое экранирование; использование системы обнаружения вторжений и пресечения попыток проникновения в операционную среду; применение мер разграничения доступа на территорию, к оборудованию и к информации в системе, в том числе мер идентификации и аутентификации пользователей и процессов; применение средств и комплексов доверенной загрузки; применение мер контроля и анализа защищенности программных и программно-аппаратных модулей системы от угроз изменения настроек и нарушения функционирования; мониторинг, регистрация и учет действий пользователей и выполнения процессов в системе; пресечение и блокирование неправомерных действий пользователей, в том числе направленных на несанкционированную инсталляцию программного обеспечения; применение мер резервирования и восстановления программного и аппаратного обеспечения системы

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В 1
Процесс определения системных требований	Частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения требований по защите конфиденциальной информации в системе или о системе)	Защита системы от вредоносного программного обеспечения; межсетевое экранирование; использование системы обнаружения вторжений и пресечения попыток проникновения в операционную среду; применение мер разграничения доступа на территорию, к оборудованию и к информации в системе, в том числе мер идентификации и аутентификации пользователей и процессов; применение средств и комплексов доверенной загрузки; применение мер контроля и анализа защищенности программных и программно-аппаратных модулей системы от угроз возможной утечки информации; мониторинг, регистрация и учет действий пользователей и выполнения процессов в системе; пресечение и блокирование неправомерных действий пользователей, направленных на копирование информации и/или несанкционированную ее передачу во внешние сети; учет, регистрация и применение технических мер защиты отчуждаемых носителей информации; применение криптографической защиты трафика как внутри системы, так и при взаимодействии ее с другими системами
	Интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований	Все способы уменьшения рисков реализации угроз безопасности информации, оцениваемых по частным показателям для данного процесса, а также: мониторинг публикаций по возможным угрозам и инцидентам безопасности информации, новым уязвимостями системного и прикладного программного обеспечения и средствам их эксплуатации в интересах учета при формировании системных требований в части защиты информации на всех стадиях жизненного цикла системы; согласование подлежащих применению на разных стадиях жизненного цикла системы мер защиты от угроз нарушения функционирования системы или утечки конфиденциальной информации; обеспечение возможности корректировки состава и характеристик мер защиты от угроз нарушения функционирования системы или ее элементов и угроз утечки информации на каждой стадии жизненного цикла системы в зависимости от фактов нарушения безопасности информации, выявленных на предыдущих стадиях
Процесс определения архитектуры системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз надежности реализации процесса определения архитектуры системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения архитектуры системы
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе определения архитектуры системы (если это возможно при управлении рисками);

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс определения архитектуры системы	Риск нарушения требований по защите информации в процессе	увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения архитектуры системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса определения архитектуры системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс определения проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса определения проекта; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе определения проекта (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения проекта
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса определения проекта и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс системного анализа	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение для каждого из системных процессов необходимых условий с завершением всех предпринимаемых действий, связанных с прогнозированием рисков, обоснованием допустимых рисков, выявлением явных и скрытых угроз, поддержкой принятия решений в жизненном цикле системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе системного анализа (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе системного анализа
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса системного анализа и защите информации в процессе, направленные на удержание рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс реализации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса реализации системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе реализации системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе реализации системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности выполнения процесса реализации системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс комплексирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса комплексирования системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе комплексирования системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе комплексирования системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса комплексирования системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс верификации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса верификации системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе верификации системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе верификации системы

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс верификации системы	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса верификации системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс передачи системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса передачи системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе передачи системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе передачи системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса передачи системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс аттестации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса аттестации системы; обеспечение готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе аттестации системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе аттестации системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса аттестации системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс функционирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз нарушения надежности реализации процесса функционирования системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики;

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В 1
Процесс функционирования системы		снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе функционирования системы; обеспечение необходимой надежности представления используемой информации; обеспечение необходимой своевременности представления используемой информации; обеспечение необходимой полноты оперативного отражения в системе новых объектов и явлений; обеспечение необходимой актуальности обновляемой информации; обеспечение необходимой безошибочности информации после контроля; обеспечение необходимой корректности обработки информации; обеспечение необходимой безошибочности действий должностных лиц
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе функционирования системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе функционирования системы; сохранение целостности системы в условиях опасных программно-технических воздействий; обеспечение защищенности активов от несанкционированного доступа; сохранение конфиденциальности используемой информации
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса функционирования системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс сопровождения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Снижение частоты возникновения источников угроз нарушения надежности реализации процесса сопровождения системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе сопровождения системы

Окончание таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные способы уменьшения рисков, используемые в результате применения методов и моделей по таблице В.1
Процесс сопровождения системы	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе сопровождения системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе сопровождения системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса сопровождения системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах
Процесс изъятия и списания системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Выполнение необходимых условий с завершением всех предпринимаемых действий процесса изъятия и списания системы; соблюдение сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Снижение частоты возникновения источников угроз нарушения требований по защите информации в процессе изъятия и списания системы (если это возможно при управлении рисками); увеличение времени развития угроз до нарушения (если это возможно при управлении рисками); оптимизация периода времени между системными диагностиками; снижение длительности системной диагностики; снижение времени восстановления системы после нарушения; выбор периода прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе изъятия и списания системы
	Интегральный риск нарушения реализации процесса с учетом требований по защите информации	Сбалансированные действия по обеспечению надежности реализации процесса изъятия и списания системы и защите информации в процессе, направленные на удержание рисков в допустимых пределах

Г.7 Материально-техническое обеспечение

В состав материально-технического обеспечения для прогнозирования рисков входят (в части, свойственной процессу управления рисками для системы):

- результаты обследования, концепция создания, технический облик и/или ТЗ на разработку для создаваемой системы, конструкторская и эксплуатационная документация для существующей системы (используют для формирования исходных данных при моделировании);
- модель угроз безопасности информации (используют для формирования необходимых исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- записи из системного журнала учета предпосылок, инцидентов и аварий при функционировании системы, связанных с нарушением требований по защите информации (используют для формирования исходных данных при моделировании);
- планы ликвидации нарушений, инцидентов и аварий, связанных с нарушением требований по защите информации, и восстановления целостности системы (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- обязанности должностных лиц и инструкции по защите информации при выполнении процесса (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);

- программные комплексы, поддерживающие применение математических моделей и методов по настоящим методическим указаниям (используют для проведения расчетов и поддержки процедур системного анализа).

Г.8 Отчетность

По результатам прогнозирования рисков составляется протокол или отчет по ГОСТ 7.32 или по форме, устанавливаемой в организации.

Примечание — Примером практического подхода к прогнозированию рисков может служить ГОСТ Р 58494, в котором положения системной инженерии изложены в приложении к системам дистанционного контроля в опасном производстве. Примеры прогнозирования рисков и решения задач системного анализа приведены в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение Д
(справочное)

Рекомендации по определению допустимых значений показателей рисков

С точки зрения остаточного риска, характеризующего приемлемый уровень целостности системы, предъявляемые требования системной инженерии подразделяют на требования при допустимых рисках, обосновываемых по прецедентному принципу согласно ГОСТ Р 59349, и требования при рисках, свойственных реальной или гипотетичной системе-эталону. При формировании требований системной инженерии необходимо обоснование достижимости целей системы и рассматриваемого процесса управления знаниями о системе, а также целесообразности использования количественных показателей рисков в дополнение к качественным показателям, определяемым по ГОСТ Р ИСО/МЭК 27005. При этом учитывают важность и критичность системы, ограничения на стоимость ее создания и эксплуатации, указывают другие условия в зависимости от специфики.

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

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

Ссылочные рекомендации по определению допустимых значений показателей для процесса управления рисками для системы отражены в таблице Д.1. При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые. В этом случае для задаваемых при моделировании условий имеет место гарантия качества и безопасности реализации системных процессов в течение задаваемого периода прогноза.

Таблица Д.1 — Ссылки для определения допустимых значений рисков

Системный процесс	Ссылки на стандарты для определения допустимых значений рисков при ориентации на обоснование по прецедентному принципу и обоснование для системы-эталона
Процессы приобретения и поставки продукции и услуг для системы	ГОСТ Р 59329—2021, приложение Г
Процесс управления моделью жизненного цикла системы	ГОСТ Р 59330—2021, приложение Г
Процесс управления инфраструктурой системы	ГОСТ Р 59331—2021, приложение Д
Процесс управления портфелем проектов	ГОСТ Р 59332—2021, приложение Г
Процесс управления человеческими ресурсами системы	ГОСТ Р 59333—2021, приложение Д
Процесс управления качеством системы	ГОСТ Р 59334—2021, приложение Г
Процесс управления знаниями о системе	ГОСТ Р 59335—2021, приложение Д
Процесс планирования проекта	ГОСТ Р 59336—2021, приложение Г
Процесс оценки и контроля проекта	ГОСТ Р 59337—2021, приложение Г
Процесс управления решениями	ГОСТ Р 59338—2021, приложение Д
Процесс управления рисками для системы	Настоящая таблица

Окончание таблицы Д.1

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

Приложение Е
(справочное)

Рекомендации по перечню методик системного анализа

Ссылочные рекомендации по перечню методик системного анализа для процесса управления рисками для системы отражены в таблице Е.1.

Таблица Е.1 — Ссылки по перечню методик системного анализа

Системный процесс	Ссылки на стандарты по перечню методик системного анализа
Процессы приобретения и поставки продукции и услуг для системы	ГОСТ Р 59329—2021, приложение Д
Процесс управления моделью жизненного цикла системы	ГОСТ Р 59330—2021, приложение Д
Процесс управления инфраструктурой системы	ГОСТ Р 59331—2021, приложение Е
Процесс управления портфелем проектов	ГОСТ Р 59332—2021, приложение Д
Процесс управления человеческими ресурсами системы	ГОСТ Р 59333—2021, приложение Е
Процесс управления качеством системы	ГОСТ Р 59334—2021, приложение Д
Процесс управления знаниями о системе	ГОСТ Р 59335—2021, приложение Е
Процесс планирования проекта	ГОСТ Р 59336—2021, приложение Д
Процесс оценки и контроля проекта	ГОСТ Р 59337—2021, приложение Д
Процесс управления решениями	ГОСТ Р 59338—2021, приложение Е
Процесс управления рисками для системы	Настоящая таблица
Процесс управления конфигурацией системы	ГОСТ Р 59340—2021, приложение Д
Процесс управления информацией системы	ГОСТ Р 59341—2021, приложение Е
Процесс измерений системы	ГОСТ Р 59342—2021, приложение Д
Процесс гарантии качества для системы	ГОСТ Р 59343—2021, приложение Е
Процесс анализа бизнеса или назначения системы	ГОСТ Р 59344—2021, приложение Д
Процесс определения потребностей и требований заинтересованной стороны для системы	ГОСТ Р 59345—2021, приложение Е
Процесс определения системных требований	ГОСТ Р 59346—2021, приложение Ж
Процесс определения архитектуры системы	ГОСТ Р 59347—2021, приложение Е
Процесс определения проекта	ГОСТ Р 59348—2021, приложение Д
Процесс системного анализа	ГОСТ Р 59349—2021, приложение Е
Процесс реализации системы	ГОСТ Р 59350—2021, приложение Д
Процесс комплексирования системы	ГОСТ Р 59351—2021, приложение Д
Процесс верификации системы	ГОСТ Р 59352—2021, приложение Д
Процесс передачи системы	ГОСТ Р 59353—2021, приложение Д
Процесс аттестации системы	ГОСТ Р 59354—2021, приложение Д
Процесс функционирования системы	ГОСТ Р 59355—2021, приложение Е
Процесс сопровождения системы	ГОСТ Р 59356—2021, приложение Е
Процесс изъятия и списания системы	ГОСТ Р 59357—2021, приложение Д

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[16] Постановление Правительства Российской Федерации от 31 декабря 2020 г. № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности»

[17] Р 50.1.053—2005 Информационные технологии. Основные термины и определения в области технической защиты информации

[18] Р 50.1.056—2005 Техническая защита информации. Основные термины и определения

[19] Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114)

[20] Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Утверждены приказом Председателя Гостехкомиссии России от 30 августа 2002 г. № 282)

[21] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17)

[22] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21)

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

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

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

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

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

Ключевые слова: актив, безопасность, защита информации, модель, процесс управления рисками, система, системная инженерия, управление

Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 11.05.2021. Подписано в печать 25.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,63.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru