ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59355— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Издание официальное

Москва
Стандартинформ
2021

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 государственным бюджетным учреждением «4 Центральный научно-исследовательский институт» Министерства обороны Российской Федерации (ФГБУ «4 ЦНИИ» Минобороны 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 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 апреля 2021 г. № 336-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

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 процессов соглашения — процессов приобретения и поставки продукции и услуг для системы — по ГОСТ Р 59329;
- для процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, управления инфраструктурой, управления портфелем, управления человеческими ресурсами, управления качеством, управления знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;
- для процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343;
- для технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, архитектуры и проекта, системного анализа, реализации, комплексирования, верификации, передачи, аттестации, 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 59356, ГОСТ Р 59357;
- для процесса функционирования системы — по настоящему стандарту.

Стандарт устанавливает основные требования системной инженерии по защите информации в процессе функционирования рассматриваемой системы и специальные требования к используемым количественным показателям.

Для планируемого и реализуемого процесса функционирования системы применение настоящего стандарта обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

System engineering. Protection of information in system operation process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа для процесса функционирования системы применительно к вопросам защиты информации для систем различных областей приложения.

Для практического применения в приложениях А—Д к настоящему стандарту приведены примеры перечней активов, подлежащих защите, и угроз, типовые модели и методы прогнозирования рисков, методические указания по прогнозированию рисков и допустимые значения для показателей рисков, примерный перечень 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) и эксплуатации систем и реализующими процесс функционирования этих систем, а также уполномоченными заинтересованными сторонами, осуществляющими 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 2.102 Единая система конструкторской документации. Виды и комплектность конструкторских документов

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

ГОСТ 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

Издание официальное

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

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

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

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

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

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

ГОСТ Р ИСО 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 20000-1 Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 59357 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 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

актив: Что-либо, что имеет ценность для организации.

Примечание — Имеются различные типы активов:
- информация;
- программное обеспечение;
- материальные активы, например, компьютер;
- услуги;
- люди и их квалификация, навыки и опыт;
- нематериальные активы, такие как репутация и имидж.

[ГОСТ Р ИСО/МЭК 27000—2012, пункт 2.3]

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.3

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]

3.1.4

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]

3.1.5

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]

3.1.6

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]

3.1.7

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

3.1.9 **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 взаимодействующие подсистемы, процесс, функциональные действия процесса, множество активов и/или выходных результатов процесса или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях.

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

3.1.11 **несанкционированное информационно-техническое воздействие на систему:** Целенаправленное программно-аппаратное и/или программное воздействие, приводящее к нарушению требуемой устойчивости функционирования системы или к несанкционированному воздействию на информацию.

3.1.12

несанкционированное воздействие на информацию: Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

[ГОСТ Р 50922—2006, статья 2.6.6]

3.1.13

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.14

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.15

пользователь: Лицо или группа лиц, извлекающих пользу из системы в процессе ее применения.

Примечание — Роль пользователя и роль оператора может выполняться одновременно или последовательно одним и тем же человеком или организацией.

[ГОСТ Р 57193—2016, пункт 4.1.50]

3.1.16

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.
[ГОСТ Р 51898—2002, пункт 3.2]

3.1.17

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

Примечания

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

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

[ГОСТ Р 57193—2016, пункт 4.1.44]

3.1.18 **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.

3.1.19

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]

3.1.20 **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.

3.1.21

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]

3.1.22 **устойчивость функционирования системы в условиях несанкционированных информационно-технических воздействий:** Способность системы сохранять на заданном интервале времени допустимые значения параметров и показателей, определяющих приемлемое функционирование системы при реализации несанкционированных информационно-технических воздействий.

Примечание — Устойчивость функционирования системы в условиях несанкционированных информационно-технических воздействий достигается путем надежной реализации процесса функционирования системы с учетом требований по защите информации. Проверяется с помощью технологических стендов или стендовых полигонов, имитирующих условия несанкционированных информационно-технических воздействий.

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

3.1.24

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.1.25 **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 функционирования системы

4.1 Общие положения

Организации используют процесс функционирования системы в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения ее результативности.

В процессе функционирования 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 нарушения надежности реализации 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 функционирования 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. Количественную оценку рисков, свойственных рассматриваемому процессу, 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 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349. При этом учитывают специфику рассматриваемой системы (см., например, [21]—[26]).

4.2 Стадии и этапы жизненного цикла системы

Процесс функционирования системы используют на стадиях эксплуатации и сопровождения системы для применения системы по назначению. Этапы работ устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень конкретных работ 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 функционирования системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.3 Цель процесса функционирования системы и назначение мер защиты информации

4.3.1 Определение целей процесса функционирования 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 с учетом специфики рассматриваемой системы.

В общем случае главная цель процесса функционирования системы состоит в ее применении по назначению. Чтобы поддерживать применение системы по назначению, в процессе ее функционирования определяют и анализируют приемлемость эксплуатационных и прогнозируемых значений параметров и показателей, а также отклонений относительно действующих соглашений, ограничений и требований заинтересованных сторон.

4.3.2 Меры защиты информации в процессе функционирования системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер защиты 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 рассматриваемой системы и реализуемой стадии жизненного цикла.

Примечание — К мерам защиты информации относятся упоминаемые далее в тексте стандарта меры периодической диагностики и восстановления возможностей по обеспечению выполнения требований защиты информации, меры противодействия угрозам, меры по снижению рисков, а также корректирующие меры.

4.3.3 Для получения близкой к реальности статистики, необходимой для обоснования применяемых мер защиты информации, используют технологические стенды или стендовые полигоны. С их помощью получают оценки достижимых показателей защищенности информации и устойчивости функционирования систем в условиях несанкционированных информационно-технических воздействий. Стендовые испытания систем осуществляют по методикам, предусматривающим имитацию условий несанкционированных информационно-технических воздействий, выявление уязвимостей, многовариантный выбор организационно-технических мер обеспечения информационной безопасности и оценку способности выполнять и восстанавливать процессы функционирования системы. Для обеспечения приемлемого функционирования системы выявляемые уязвимости подлежат контролю и последующему устранению (если такое устранение возможно и экономически целесообразно).

4.4 Основные принципы системного анализа

При проведении системного анализа процесса функционирования 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 в планируемых и реализуемых процессах на протяжении всего жизненного цикла системы.

4.5 Основные усилия по обеспечению защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе функционирования 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 функционирования 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 поставля-

емые 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).

Примечание — Если информация относится к категории государственной тайны, в вопросах защиты информации руководствуются регламентирующими документами соответствующих государственных регуляторов.

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

Требования системной инженерии по защите информации в процессе функционирования системы включают:

- требования к составам 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 процесса, обоснованию эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

5.3 Состав выходных результатов и выполняемых действий в процессе функционирования 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 ИСО/МЭК 20000-1, ГОСТ Р 51904, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193 с учетом специфики рассматриваемой системы.

Примечание — В процессе функционирования системы необходимо учитывать решение таких вопросов как:

- гарантированное подтверждение достаточности автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации);
- учет возможности повышения уровня конфиденциальности данных в процессе их обработки в системах искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации и т. п.);
- регламентация вопросов обеспечения конфиденциальности тестовых выборок исходных данных, используемых испытательными лабораториями при оценке соответствия прикладных систем искусственного интеллекта, с сохранением прозрачности и подотчетности этого процесса.

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 функционирования 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 обеспечивающих систем.

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 требований 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, [20]—[24].

Примеры перечней учитываемых активов и угроз в процессе функционирования системы приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процесса функционирования системы 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 функционирования системы осуществляют с использованием методов, моделей и методических указаний, представленных в приложениях В, Г, Д, с учетом ре-

комендаций 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.

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 процесса функционирования системы определен в 6.3.

Типовые методы и модели для процесса функционирования системы, методические указания по прогнозированию рисков, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д, Е. Характеристики мер защиты информации 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 функционирования 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 функционирования системы являются:

- ограничения в применении системы, которые влияют на системные требования, архитектуру и/или проекты, связанные с системой;
- доступ к обеспечивающим системам, услугам и материалам, необходимым для функционирования рассматриваемой системы;
- обученные и компетентные операторы системы;
- непосредственно продукция и/или услуги системы, отвечающие требованиям заинтересованных сторон (продукция может быть как материальной, так и нематериальной, например, информационной продукцией, или их комбинацией);
- результаты контроля функционирования системы, в том числе состояния защиты циркулирующей в ней информации;
- карта двунаправленной прослеживаемости возможностей системных элементов, участвующих в процессе функционирования системы, относительно выполнения системных требований и требований заинтересованных сторон системы;
- результаты поддержки конкретных заинтересованных сторон.

6.1.3 Для получения выходных результатов процесса функционирования системы в общем случае выполняют следующие основные действия:

- подготовительные действия:
  - определение стратегии эксплуатации системы, включая определение критериев и методов обеспечения качества производимой продукции и/или услуг, способов организации приемлемого функционирования и реагирования на отклонения, методов защиты окружающей среды, технологий обеспечения устойчивости и безопасности функционирования системы,
  - определение ограничений в применении системы, которые влияют на системные требования, архитектуру и/или проекты, связанные с системой,
  - определение и планирование действий относительно необходимых обеспечивающих систем, услуг и материалов, необходимых для поддержки функционирования рассматриваемой системы, и обеспечение доступа к ним,

- определение требований к квалификации и обучению персонала, прием на работу и возложение обязанностей на обученных и компетентных операторов рассматриваемой и обеспечивающих систем;

- действия по обеспечению функционирования и управлению процессом, включая:

- применение системы по ее целевому назначению в заданных условиях эксплуатации согласно требованиям заинтересованных сторон,

- применение материалов и иных ресурсов, необходимых для производства продукции и/или оказания услуг системой, для управления системой и поддержки процесса функционирования системы,

- контроль функционирования системы, включая поддержку стратегии эксплуатации системы, сравнительное сопоставление затрат и ущербов с целями и ограничениями в применении системы,

- регистрацию эксплуатационных инцидентов, случаев отклонений от приемлемого функционирования системы, выявление проблем в обеспечении приемлемого функционирования, реагирование на инциденты и отклонения и восстановление приемлемого функционирования системы,

- анализ данных по инцидентам, выявленным проблемам и отклонениям от приемлемого функционирования системы для определения их первопричин, прогнозирования рисков и принятия упреждающих мер по обеспечению безопасности и улучшению процесса функционирования системы,

- поддержку двунаправленной прослеживаемости возможностей системных элементов, участвующих в процессе функционирования системы, относительно системных требований и требований заинтересованных сторон;

- действия по поддержке конкретных заинтересованных сторон, включая обеспечение им помощи и консультаций и определение степени их удовлетворенности.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процесса функционирования системы, 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 возможных ущербов (см. приложения В, Г).

6.2 Требования к составу показателей

Выбираемые показатели должны позволять проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения надежности реализации процесса функционирования 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 корректирующие меры. Дополнительно могут быть использованы вспомогательные статистические показатели, характеризующие события, которые уже произошли, и их влияние на эффективность защиты информации при реализации процесса. 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 прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе функционирования системы используют следующие количественные показатели:

- риск нарушения надежности реализации процесса функционирования системы без учета требований по защите информации;

- риск нарушения требований по защите информации в процессе функционирования системы;

- интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации.

Примечание — Дополнительно могут быть использованы другие показатели, например, коэффициент оперативной готовности системы и/или вероятность нарушения устойчивости функционирования системы в условиях информационно-технических воздействий.

6.3.2 Риск нарушения надежности реализации процесса функционирования системы без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса в сопоставлении с возможным ущербом.

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

6.3.4 Интегральный риск нарушения реализации процесса функционирования системы 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 (см. В.2, В.3, В.4) в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

- временные данные функционирования системы защиты информации, в т. ч. срабатывания ее исполнительных механизмов (могут быть использованные данные, полученные при верификации и аттестации системы);
- 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, в т. ч. данные о событиях, связанных 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 о результатах 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 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 приведены в приложении В.

7 Требования к системному анализу

Требования к системному анализу процесса функционирования системы включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в процессе функционирования системы.

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

При обосновании и формулировании требований к системному анализу дополнительно руководствуются рекомендациями 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 рассматриваемой системы (см., например, [21] — [26]).

Примечание — Примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, 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 59349, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе функционирования 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 (по [21]—[24]);
- договоры и соглашения на проведение работ по эксплуатации и сопровождению системы;
- финансовые и плановые документы, связанные с эксплуатацией и сопровождением системы;
- документацию при выполнении научно-исследовательских работ (по ГОСТ 7.32, ГОСТ 15.101) с учетом специфики применяемой системы;
- конструкторскую и технологическую документацию для применяемой системы (по ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201);
- эксплуатационную и ремонтную документацию (по ГОСТ 2.602, ГОСТ 34.201, ГОСТ Р 2.601) с учетом специфики применяемой системы;
- документацию системы менеджмента качества организации, эксплуатирующей систему (по ГОСТ Р ИСО 9001);
- технические задания (по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839) с учетом специфики применяемой системы и планов ее модернизации и развития;
- 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 функционирования 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 и ГОСТ Р 51275);
- угрозы государственным информационным системам, информационным системам персональных данных, автоматизированным системам 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, значимым объектам критической информационной инфраструктуры Российской Федерации (по [21]—[24]);
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы (по ГОСТ Р ИСО/МЭК 27002 и 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, угрозы возникновения ущерба репутации и/или потери доверия поставщика к конкретному приобретателю, информация и информационные системы которого были скомпрометированы (по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С, ГОСТ Р 59215);
- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги (по ГОСТ Р ИСО/МЭК 27036-4);
- прочие соответствующие угрозы безопасности информации и уязвимости 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

В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе функционирования системы применяют любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. С учетом набираемой статистики в настоящем стандарте типовые модели и методы системного анализа обеспечивают оценку следующих показателей (согласно 6.3):

- риска нарушения надежности реализации процесса функционирования системы без учета требований по защите информации (см. В.2);
- риска нарушения требований по защите информации в процессе функционирования системы (см. В.3);
- интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации (см. В.4).

Риски определяют соответствующими вероятностными показателями в сопоставлении с возможным ущербом. Вероятностные оценки обеспечивают уровень адекватности, достаточный для решения задач системного анализа, при условии многократной повторяемости анализируемых событий или в предположении такой повторяемости.

Примечание — Для имитируемых условий несанкционированных информационно-технических воздействий показатели риска нарушения надежности реализации процесса функционирования системы без учета и с учетом требований по защите информации могут быть интерпретированы как соответствующие показатели устойчивости функционирования системы.

В.1.2 В общем случае в целях моделирования полагают, что система реализует M функций, связанных с производством продукции или оказанием услуг, $M \geq 1$. Вместе с тем, с точки зрения системного анализа для выявления закономерностей функции могут быть сгруппированы с учетом похожих технологий их выполнения. Поэтому для уменьшения методической громоздкости, связанной с индексированием каждой из функций в В.2 — В.4 приведены рекомендации с ориентацией на отдельную функцию или объединенное множество функций без их дифференциации по отдельным функциям. При необходимости детального учета каждой m-й функции ($m = 1,\ldots, M$) рекомендации даны в Г.4.

В.1.3 Для расчета типовых показателей рисков исследуемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. Модели и методы системного анализа таких систем используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, данные собираемой и накапливаемой статистики по процессам и возможным условиям их реализации.

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

В.1.4 При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных событий (состояний). Это пространство элементарных событий формируют в результате статистического анализа произошедших событий с их привязкой ко временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если…», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя процессов может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования моделируемой системы. Применительно к анализируемому сценарию модели ориентированы на расчет вероятности определенного элементарного события в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.1.5 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований по защите информации в системе (в качестве моделируемой системы простой или сложной структуры могут быть рассмотрены выходные результаты с задействованными активами и действия процесса, к которым предъявлены определенные требования, включая требования по защите информации);
- в условиях неопределенностей возникновение и разрастание различных угроз описывается в терминах случайных событий;
- для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и/или защитных преград, предназначенных для воспрепятствования реализации угроз.

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение реализации рассматриваемого процесса.

В.1.6 В общем случае выполнение или невыполнение задаваемых условий при проведении системного анализа отслеживается с использованием индикаторной функции *Ind* (α), которая позволяет учесть ограничения на допустимые риски и, при необходимости, последствия, связанные с нарушениями условий:

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

где *R* — расчетное значение конкретного вероятностного показателя, сравниваемого с его задаваемым допустимым значением.

Выполнение условия α логически означает, что соответствующий риск находится в допустимых пределах.

В.1.7 В В.2 приведены математические модели и методы для прогнозирования риска нарушения надежности реализации процесса функционирования системы без учета требований по защите информации, в В.3 — методы для прогнозирования риска нарушения требований по защите информации, в В.4 — методы оценки интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации.

В.1.8 Для моделируемой системы сложной структуры применимы методы, изложенные в В.2.4, включая методы комбинации и повышения адекватности моделей.

В.1.9 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы или для системы, выбранной в качестве аналога. Для исследования запроектных сценариев при моделировании могут быть использованы гипотетичные исходные данные.

В приложении Г изложены методические указания по прогнозированию рисков для процесса функционирования системы.

В.1.10 Другие возможные подходы для оценки рисков описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59349, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

В.2 Математические модели и методы для прогнозирования риска нарушения надежности реализации процесса функционирования системы без учета требований по защите информации

В.2.1 Общие положения

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

Примечание — Выполнение требований по защите информации в В.2 не рассматривается (учет этих требований см. в В.3 и В.4).

В.2.1.2 При выполнении каждой *m*-й функции системы ($m = 1,\ldots, M$) для выбора соответствующей модели возможен один из трех вариантов.

Для варианта 1 результат выполнения функции зависит лишь от случайных событий, связанных с возникновением технических отказов, и не зависит от качества используемой информации (или информация не используется, или ее качество заведомо приемлемо для выполнения функции). Этот вариант свойственен производству сугубо материальной продукции, например, технических деталей, трубной или пластиковой продукции, пиломатериалов, обычных электрических инструментов.

Для варианта 2 результатом выполнения функции является информация, т. е. надежность реализации функции в полной мере определяется надежностью и своевременностью представления, полнотой и достоверностью используемой информации, а также безошибочностью действий должностных лиц. Этот вариант свойственен информационным системам, различным автоматизированным системам управления, системам производства информационной продукции.

Вариант 3 является комбинацией двух первых вариантов, т. е. результат выполнения функции зависит не только от случайных событий, связанных с возникновением технических отказов, но и от качества используемой информации. Этот вариант свойственен, например, системам автоматизированного производства, робототехническим системам, системам искусственного интеллекта или иным кибернетическим системам.

В.2.1.3 В моделях для варианта 1 под моделируемой системой понимается отдельное действие или множество действий процесса функционирования системы, получаемый выходной результат или множество выходных результатов. Модели для варианта 2 позволяют оценить качество используемой информации, они применимы к каждому из действий или каждому из выходных результатов или их множеству в условиях, когда это уместно с точки зрения системного анализа. При моделировании процесса в качестве системных элементов могут фигурировать иные сущности, подлежащие учету в моделируемой системе. Модели для варианта 3 являются комбинациями моделей для первых двух вариантов.

В.2.1.4 В В.2.2—В.2.4 описаны модели и методы прогнозирования рисков в системе, представляемой в виде «черного ящика», в системах сложной структуры, рекомендации по комбинации и повышению адекватности моделей. В В.2.5 и 2.6 представлены рекомендации по методам анализа соответственно для вариантов 2 и 3 выполнения функций процесса функционирования системы.

В.2.1.5 В общем случае для каждого из анализируемых действий или выходных результатов процесса функционирования системы, являющихся элементом в моделируемой системе простой или сложной структуры, возможно либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения этого действия или получения выходного результата с устранением выявляемых отклонений и нарушений.

В.2.1.6 В терминах системы, состоящей из элементов, отождествляемых с выполняемыми действиями или получаемыми выходными результатами, под целостностью моделируемой системы понимается такое состояние элементов модели системы, которое в течение задаваемого периода прогноза отвечает требованию обеспечения надежной реализации процесса функционирования системы. С точки зрения вероятностного прогнозирования риска нарушения надежности реализации процесса пространство элементарных событий отдельного действия или выходного результата (элемента моделируемой системы) на временной оси образуют следующие основные состояния:

- «Целостность элемента моделируемой системы сохранена», если в течение всего периода прогноза обеспечена надежная реализация анализируемого действия или получения определенного выходного результата процесса функционирования системы;
- «Целостность элемента моделируемой системы нарушена» — в противном случае.

Надежность реализации процесса функционирования системы в течение задаваемого периода прогноза обеспечена, если в течение этого периода для всех элементов моделируемой системы (т. е. для всех осуществляемых действий или получаемых выходных результатов, логически объединяемых условием «И») обеспечена их целостность. Это означает, что в течение периода прогноза для всех осуществляемых недублируемых действий будет наблюдаться элементарное состояние «Целостность элемента моделируемой системы сохранена». При дублировании действия с помощью нескольких элементов надежность реализации действия (как подсистемы из дублируемых элементов) считается обеспеченной в течение задаваемого периода прогноза, если в течение этого периода хотя бы для одного элемента этой подсистемы наблюдается элементарное состояние «Целостность элемента моделируемой системы сохранена».

В.2.1.7 Оценки осуществляют с использованием вероятностных показателей нахождения моделируемой системы в определенном элементарном состоянии. В сопоставлении с возможным ущербом вероятность нахождения в состоянии «Целостность элемента моделируемой системы нарушена» характеризует риск нарушения надежности выполнения соответствующего действия или получения соответствующего выходного результата реализуемого процесса функционирования системы.

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

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

Модель представляет собой частный случай модели В.2.3, если период между контролями состояния системы больше периода прогноза. Учитывая это, для расчетов по данной модели используют формулы (В.2)—(В.7) из В.2.3. Модель применима на практике лишь для оценки и сравнения случая полностью бесконтрольного функционирования моделируемой системы (например, там, где контроль невозможен или нецелесообразен по функциональным, экономическим или временным соображениям), а также когда ответственные лица пренебрегают функциями контроля или не реагируют должным образом на результаты контроля.

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

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

Примечание — Моделируемая система в виде «черного ящика» представляет собой единственный элемент.

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

В рамках модели развитие событий в системе считается не нарушающим надежность реализации процесса функционирования системы в течение заданного периода прогноза, если к началу этого периода требуемые условия для реализации процесса обеспечены и в течение всего периода либо источники угроз не активизируются,

либо после активизации происходит их своевременное выявление и принятие адекватных мер противодействия угрозам. В целях моделирования предполагают, что существуют не только средства контроля (диагностики) состояния реализуемого процесса функционирования системы, но и способы поддержания и/или восстановления возможностей по выполнению процесса при выявлении источников, признаков или следов активизации угроз (к таковым могут быть отнесены выявляемые отклонения от приемлемого функционирования рассматриваемой системы или ее элементов). Восстановление осуществляется лишь в период системного контроля. Соответственно, чем чаще осуществляют системный контроль с должной своевременной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии обеспечения надежности реализации процесса функционирования системы из-за возможных угроз в период прогноза (так как в принятой модели за счет предупреждающих действий по результатам диагностики устраняются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент нанесения ущерба от реализации какой-либо угрозы).

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

Примечание — Если активизация мгновенная, это считают эквивалентным внезапному отказу. Усилия системной инженерии как раз и направлены на использование времени постепенной активизации угроз для своевременного выявления, распознавания (в т. ч. на уровне предпосылок) и противодействия угрозам.

Надежность реализации процесса функционирования системы считается нарушенной лишь после того, как активизация источника угрозы происходит за период прогноза (т. е. возникает переход в элементарное состояние «Целостность элемента моделируемой системы нарушена»). В рамках принятой формализации при отсутствии нарушений результатом применения очередной системной диагностики является подтверждение возможностей по реализации процесса, а при наличии нарушений перед диагностикой результатом применения очередной системной диагностики является полное восстановление до приемлемого уровня нарушенных возможностей реализации процесса.

С математической точки зрения модель позволяет оценить вероятностное значение риска нарушения надежности реализации процесса функционирования системы в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели является расчетная вероятность нарушения надежности реализации процесса функционирования системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики) целостности системы.

Для расчета риска нарушения надежности реализации процесса функционирования системы исходные данные формально определяют применительно к выполняемым действиям процесса, выходным результатам и защищаемым активам следующим образом:

σ — частота возникновения источников угроз в моделируемой системе с точки зрения нарушения надежности реализации процесса функционирования системы;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности (выполняемых действий процесса, выходных результатов или защищаемых активов, используемых при выполнении действия), т. е. до нарушения надежности реализации процесса;

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

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

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы (учитывают путем использования способа 4 из В.2.4);

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

Примечание — Примеры переопределения этих исходных данных (согласно способу 1 из В.2.4), конкретизированные в приложении к выходным результатам и действиям процесса функционирования системы, приведены в Г.4.

Оценку вероятности $R_{надежн}(T_{зад})$ нарушения надежности реализации процесса функционирования системы в течение периода прогноза $T_{зад}$ осуществляют по формуле

$$R_{надежн}(T_{зад}) = R_{надежн}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = 1 - P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}), \quad (В.2)$$

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

Примечание — В модели изложен случай, когда $T_{диаг} = T_{восст}$. Для учета более общего случая, когда средние времена системной диагностики и восстановления целостности не совпадают, используют способ 4 из В.2.4.

Возможны два случая:

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

Для случая 1 при условии независимости исходных характеристик вероятность $P_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ отсутствия нарушений надежности реализации процесса функционирования системы в течение периода прогноза $T_{зад}$ вычисляют по формуле

$$P_{возд(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1} \left\{\sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}}\right\}, & \text{если } \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{зад}} \left[1 + \sigma T_{зад}\right], & \text{если } \sigma = \beta^{-1}. \end{cases} \quad (В.3)$$

Примечание — Формулу (В.3) используют также для оценки риска отсутствия нарушений надежности реализации процесса функционирования системы при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по математической модели «черного ящика» при отсутствии какого-либо контроля (см. В.2.2).

Для случая 2 при условии независимости исходных характеристик вероятность отсутствия нарушений надежности реализации процесса функционирования системы в течение прогноза $T_{зад}$ вычисляют по формуле

$$P_{возд\,(2)} = P_{серед} \cdot P_{кон}, \quad (В.4)$$

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

$$P_{серед} = P^{N}_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}), \quad (В.5)$$

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

$P_{кон}$ — вероятность отсутствия нарушений надежности реализации процесса функционирования системы после последнего системного контроля, вычисляемая по формуле (В.3), т. е.

$$P_{кон} = P_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}), \quad (В.6)$$

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

$$T_{ост} = T_{зад} - N \cdot (T_{меж} + T_{диаг}). \quad (В.7)$$

Формула (В.4) логически интерпретируется так: для обеспечения выполнения требований по защите информации за весь период прогноза требуется обеспечение выполнения требований по реализации процесса на каждом из участков — будь то середина или конец задаваемого периода прогноза $T_{зад}$.

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

В итоге вероятность отсутствия нарушений надежности реализации процесса функционирования системы в течение периода прогноза $T_{зад}$ определяется аналитическими выражениями (В.3)—(В.7) в зависимости от соотношений между исходными данными. Это позволяет вычислить по формуле (В.2) вероятность нарушения надежности реализации процесса функционирования системы $R_{надежн}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по обеспечению выполнения процесса. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения надежности реализации процесса функционирования системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

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

В.2.4 Расчет риска для систем сложной структуры, комбинация и повышение адекватности моделей

В.2.4.1 Описанные в В.2.2 и В.2.3 модели применимы для проведения оценок, когда моделируемая система представляется в виде «черного ящика» и когда значения времен системной диагностики и восстановления нарушенной целостности совпадают. В развитие моделей В.2.2 и В.2.3 в настоящем подразделе приведены способы, позволяющие создавать модели для систем сложной структуры и более общего случая, когда значения времен системной диагностики и восстановления нарушенных возможностей системы различны.

В.2.4.2 Расчет основан на применении следующих четырех инженерных способов.

1-й способ позволяет использовать одни и те же модели для расчетов различных показателей по области их приложения. Поскольку модели математические, то путем смыслового переопределения исходных данных возможно использование одних и тех же моделей для оценки показателей, различающихся по смыслу, но идентичных по методу расчета.

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

Рисунок В.1 — Система из последовательно соединенных элементов («И»)

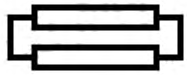

Рисунок В.2 — Система из параллельно соединенных элементов («ИЛИ»)

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

- для системы из двух последовательно соединенных элементов

$$P(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)], \quad (В.8)$$

- для системы из двух параллельно соединенных элементов

$$P(t) = P_1(t) \cdot P_2(t), \quad (В.9)$$

где $P_m(t)$ — вероятность нарушения надежности реализации процесса для m-го элемента за заданное время t, $m = 1, 2$.

Рекурсивное применение соотношений (В.8), (В.9) снизу-вверх дает соответствующие вероятностные оценки для сложной логической структуры с параллельно-последовательным логическим соединением элементов.

Примечание — Способ рекурсивного применения процессов рекомендован ГОСТ Р 57102. Рекурсивное применение снизу-вверх означает первичное применение моделей В.2.2 или В.2.3 сначала для отдельных системных элементов, представляемых в виде «черного ящика» в принятой сложной логической структуре системы, затем, учитывая характер логического объединения («И» или «ИЛИ») в принятой структуре, по формуле (В.8) или (В.9) проводится расчет вероятности нарушения надежности реализации процесса функционирования системы за

время t для объединяемых подсистем. И так — до объединения на уровне системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формуле (В.8) или (В.9) от исходных параметров моделей В.2.2 и В.2.3.

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.2.2 и В.2.3 и применения 2-го способа получается вероятность нарушения надежности реализации процесса в течение заданного периода времени t. Если для каждого элемента просчитать эту вероятность для всех точек t от нуля до бесконечности, получится траектория функции распределения времени нарушения надежности реализации процесса по каждому из элементов в зависимости от реализуемых мер контроля и восстановления целостности, т. е. то, что используется в формулах (В.8) и (В.9). Полученный вид этой функции распределения, построенной по точкам (например, с использованием программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения надежности реализации процесса каждого из элементов и системы в целом. С точки зрения системной инженерии это среднее время интерпретируют как виртуальную среднюю наработку на нарушение надежности реализации процесса функционирования системы при прогнозировании риска по моделям В.2.2 и В.2.3 для системы простой и сложной структуры. Обратная величина этого среднего времени является частотой нарушений надежности реализации процесса в условиях определенных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения процесса для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей В.2.2 и В.2.3 или аналогичных им для расчетов по моделям «черного ящика». Этот способ используют, когда изначальная статистика для определения частоты отсутствует или ее недостаточно.

4-й способ в дополнение к возможностям 2-го и 3-го способов повышает адекватность моделирования за счет развития моделей В.2.2 и В.2.3 в части учета времени на восстановление после нарушения надежности реализации процесса. В моделях В.2.2 и В.2.3 время системного контроля по составному элементу одинаково и равно в среднем $T_{диаг}$. Вместе с тем, если по результатам контроля требуются дополнительные меры для восстановления нарушенных возможностей по выполнению процесса в течение времени $T_{восст}$, то для расчетов усредненное время контроля $T_{диаг}$ должно быть изменено. При этом усредненное время контроля вычисляют итеративно с заданной точностью:

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

$$T_{диаг}^{(2)} = T_{диаг}^{(1)} \cdot \left(1 - R^{(1)}\right) + R^{(1)} \cdot T_{восст}, \tag{В.10}$$

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

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

$$T_{диаг}^{(r)} = T_{диаг}^{(r-1)} \cdot \left(1 - R^{(r-1)}\right) + R^{(r-1)} \cdot T_{восст}, \tag{В.11}$$

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

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

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

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

- $T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы;
- $T_{восст}$ — среднее время восстановления нарушенной целостности моделируемой системы.

В итоге с использованием моделей и методов В.2.2—В.2.4 осуществляется расчет вероятности нарушения надежности реализации процесса $R_{\text{надежн}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$, более общий по сравнению с расчетом $R_{\text{надежн}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$, производимым по формуле (В.2), за счет возможности учета различий в параметрах $T_{\text{диаг}}$ и $T_{\text{восст}}$

Примечание — Способ итеративного применения процессов рекомендован ГОСТ Р 57102, адаптированный вариант этого способа приведен в ГОСТ Р 58494.

В.2.4.3 Применение инженерных способов 1—4 обеспечивает более точный прогноз вероятности нарушения требований для системы сложной структуры с учетом различий во временах диагностики и восстановления целостности моделируемой системы.

В.2.4.4 Для применения результатов моделирования в оценках обобщенного риска нарушения надежности реализации процесса функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $R_{\text{доп надежн}}(T_{\text{зад}})$ и условие надежности реализации процесса α: $R_{\text{надежн}}(T_{\text{зад}}) < R_{\text{доп надежн}}(T_{\text{зад}})$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Этот учет осуществляют с помощью индикаторного коэффициента $Z_{\text{надежн -1}}(T_{\text{зад}})$ надежности реализации процесса в системе

$$Z_{\text{надежн -1}}(T_{\text{зад}}) = \begin{cases} 1, & \text{если условие надежности реализации процесса в системе } \alpha \text{ выполнено,} \\ 1 - R_{\text{надежн}}(T_{\text{зад}}), & \text{если условие } \alpha \text{ не выполнено или не задано,} \end{cases} \quad (\text{В.12})$$

где $R_{\text{надежн}}(T_{\text{зад}}) = R_{\text{надежн}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$.

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы коэффициента $[1 - Z_{\text{надежн -1}}(T_{\text{зад}})]$ как риск нарушения надежности реализации процесса функционирования системы по варианту 1 выполнения функций.

Примечание — При наличии статистических данных в дополнение к рекомендуемым в настоящем стандарте методам и моделям или в комбинации с ними для расчетов могут быть использованы иные приемлемые методы, например, методы оценки рисков нарушения надежности реализации процесса аттестации системы (см. ГОСТ Р 59354).

Детальный учет особенностей процесса функционирования системы по варианту 1 выполнения функций осуществляют на уровне соответствующих методик системного анализа (см. приложение Е).

В.2.5 Расчет вероятностных показателей качества используемой информации

В.2.5.1 В подразделе представлены способы расчета вероятностных показателей качества информации, используемой в процессе функционирования системы. Их применение позволяет проводить прогнозирование рисков по варианту 2, когда результатом выполнения функции является информация (см. В.2.1). Согласно ГОСТ Р 59341 при выполнении таких функций требуется обеспечить надежность и своевременность представления, полноту, достоверность и безопасность используемой информации. Достоверность выходной информации определяется истинностью исходных данных, безошибочностью входной информации, корректностью обработки, безошибочностью при хранении и передаче информации и сохранением ее актуальности на момент использования.

В.2.5.2 В основе прогнозирования рисков по варианту 2 положены модели ГОСТ Р 59341, предназначенные для оценки:

- надежности представления используемой информации;
- своевременности представления используемой информации;
- полноты оперативного отражения в системе новых объектов и явлений;
- актуальности обновляемой информации;
- безошибочности информации после контроля;
- корректности обработки информации;
- безошибочности действий должностных лиц.

Примечание — Дополнительно в разделе В.3 настоящего стандарта рекомендованы математические модели ГОСТ Р 59341, предназначенные для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенности активов от несанкционированного доступа, сохранения конфиденциальности используемой информации.

В.2.5.3 Применение моделей для оценки надежности представления используемой информации (см. ГОСТ Р 59341—2021, В.3.2 приложения В) позволяет оценить вероятность надежного представления информации в системе в течение заданного периода прогноза $P_{\text{над предст}}(T_{\text{зад}})$. Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{\text{доп над}}(T_{\text{зад}})$ и условие надежности представления информации α: $P_{\text{над предст}}(T_{\text{зад}}) \geq P_{\text{доп над}}(T_{\text{зад}})$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Расчет осуществляют с использованием коэффициента надежности представления информации $Z_{\text{над предст}}(T_{\text{зад}})$ аналогично В.2.4.4

$$Z_{\text{над предст}}(T_{\text{зад}}) = \begin{cases} 1, \text{ если условие надежности предоставления информации } \alpha \text{ выполнено,} \\ P_{\text{над предст}}(T_{\text{зад}}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (B.13)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента [1 – $Z_{\text{над предст}}(T_{\text{зад}})$] как риск нарушения надежности представления информации в системе.

В.2.5.4 Применение модели для оценки своевременности представления используемой информации (см. ГОСТ Р 59341—2021, В.3.3 приложения В) позволяет оценить вероятностно-временные показатели обработки информации различных типов и интегрирующие показатели — относительную долю своевременно обработанных запросов лишь тех типов, для которых выполняются требования по своевременности $C_{\text{своевр}}$, и коэффициент своевременности обработки запросов $Z_{\text{своевр}}$.

Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) в приложении к каждому из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) задают требования к своевременности обработки запросов в виде одного из двух критериев, определяющих с учетом возможных ущербов условие своевременности представления информации α:

- критерия своевременности по среднему времени реакции (среднее время реакции системы при обработке запросов конкретного типа должно быть не более задаваемого — условие своевременности α_1);
- вероятностного критерия (вероятность своевременной обработки запросов конкретного типа в системе за заданное время должна быть не ниже задаваемой — условие своевременности α_2).

Тем самым условие своевременности представления информации α формулируют в виде условий α_1 или α_2 с добавлением, что в случае их нарушения возможный ущерб не должен превышать допустимого.

Применение результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации осуществляют с помощью коэффициента своевременности обработки запросов $Z_{\text{своевр}}$

$$Z_{\text{своевр}} = \begin{cases} 1, \text{ если условия своевременности } \alpha \text{ выполнены для всех типов запросов,} \\ C_{\text{своевр}}, \text{ если хотя бы одно условие своевременности } \alpha \text{ не выполнено.} \end{cases} \quad (B.14)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента (1 – $Z_{\text{своевр}}$) как риск нарушения своевременности представления используемой информации в системе.

В.2.5.5 Применение модели для оценки полноты оперативного отражения в системе новых объектов и явлений (см. ГОСТ Р 59341—2021, В.3.4 приложения В) позволяет оценить вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{\text{полн}}$. Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{\text{доп полн}}$ и условие полноты оперативного отражения в системе новых объектов и явлений α: $P_{\text{полн}} \geq P_{\text{доп полн}}$ с дополнением — возможный ущерб не должен превышать допустимого. Расчет осуществляют с помощью коэффициента полноты оперативного отражения в системе новых объектов и явлений $Z_{\text{полн}}$

$$Z_{\text{полн}} = \begin{cases} 1, \text{ если условие полноты отражения в системе объектов и явлений } \alpha \text{ выполнено,} \\ P_{\text{полн}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (B.15)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента (1 – $Z_{\text{полн}}$) как риск нарушения полноты оперативного отражения в системе новых объектов и явлений.

В.2.5.6 Применение модели для оценки актуальности обновляемой информации (см. ГОСТ Р 59341—2021, В.3.5 приложения В) позволяет оценить вероятность сохранения актуальности информации в системе на момент ее использования $P_{\text{акт}}$. Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{\text{доп акт}}$ и условие сохранения актуальности информации в системе на момент ее использования α: $P_{\text{акт}} \geq P_{\text{доп акт}}$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Расчет осуществляют с помощью коэффициента актуальности информации в системе $Z_{\text{акт}}$

$$Z_{\text{акт}} = \begin{cases} 1, \text{ если условие сохранения актуальности информации в системе } \alpha \text{ выполнено,} \\ P_{\text{акт}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (B.16)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы коэффициента актуальности информации (1 – $Z_{\text{акт}}$) как риск нарушения актуальности информации в системе на момент ее использования.

В.2.5.7 Применение модели для оценки безошибочности информации после контроля (см. ГОСТ Р 59341—2021, В.3.6 приложения В) позволяет оценить вероятность отсутствия ошибок в информации после ее контроля $P_{безош}$. Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{доп\ безош}$ и условие обеспечения безошибочности информации после контроля α: $P_{безош} \geq P_{доп\ безош}$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Расчет осуществляют с помощью коэффициента безошибочности информации в системе $Z_{безош}$

$$Z_{безош} = \begin{cases} 1, \text{ если условие безошибочной информации после контроля } \alpha \text{ выполнено,} \\ P_{безош}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.17)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{безош})$ как риск нарушения безошибочности информации в системе после ее контроля.

В.2.5.8 Применение модели для оценки корректности обработки информации (см. ГОСТ Р 59341—2021, В.3.7 приложения В) позволяет оценить вероятность получения корректных результатов обработки информации $P_{корр}$. Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{доп\ корр}$ и условие обеспечения корректности обработки информации α: $P_{корр} \geq P_{доп\ корр}$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Расчет осуществляют с помощью коэффициента корректности обработки информации в системе $Z_{корр}$

$$Z_{корр} = \begin{cases} 1, \text{ если условие обеспечения корректности обработки информации } \alpha \text{ выполнено,} \\ P_{корр}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.18)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{корр})$ как риск нарушения корректности обработки информации в системе.

В.2.5.9 Применение моделей для оценки безошибочности действий должностных лиц (см. ГОСТ Р 59341—2021, В.3.8 приложения В) позволяет оценить воздействие «человеческого фактора» на качество используемой информации на уровне вероятности безошибочных действий должностных лиц в течение заданного периода прогноза $P_{чел}(T_{зад})$.

Примечание — Определение ошибки и влияние человеческого фактора на надежность рекомендуется выполнять по ГОСТ Р 59333, ГОСТ Р МЭК 62508.

Для применения результатов моделирования в оценках обобщенного риска нарушения качества используемой информации в процессе функционирования системы без учета требований по защите информации (см. В.2.6) задают допустимый уровень $P_{доп\ чел}(T_{зад})$ и условие безошибочности действий должностных лиц α: $P_{чел}(T_{зад}) \geq P_{доп\ чел}(T_{зад})$ с дополнением — возможный ущерб от нарушения не должен превышать допустимого. Расчет осуществляют с помощью коэффициента безошибочных действий должностных лиц $Z_{чел}(T_{зад})$

$$Z_{чел}(T_{зад}) = \begin{cases} 1, \text{ если условие безошибочности действий должностных лиц } \alpha \text{ выполнено,} \\ P_{чел}(T_{зад}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.19)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $[1 - Z_{чел}(T_{зад})]$ как риск нарушения безошибочности действий должностных лиц в системе.

В.2.5.10 Показатель обобщенного риска нарушения надежности реализации процесса функционирования системы по варианту 2 выполнения функций в силу своей специфики совпадает с риском нарушения качества используемой информации в процессе функционирования системы (см. В.2.1.2) и позволяет оценить свойства процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях реализации с обеспечением надежности и своевременности представления, полноты и достоверности информации и безошибочности действий должностных лиц (без учета требований по защите информации). Обобщенный риск используют для сравнения весомости прогнозируемых частных рисков, выявления явных и скрытых угроз и поддержки принятия решений для задач системного анализа согласно разделу 7 и ГОСТ Р 59349.

В сопоставлении с возможным ущербом обобщенный риск нарушения качества используемой информации в процессе функционирования системы $Z_{обобщен\ -2}(T_{зад})$ для периода прогноза $T_{зад}$ по варианту 2 выполнения функций без учета требований по защите информации определяют по формуле

$$Z_{обобщен\ -2}(T_{зад}) = 1 - Z_{над\ предст}(T_{зад}) \cdot Z_{своевр} \cdot Z_{полн} \cdot Z_{акт} \cdot Z_{безош} \cdot Z_{корр} \cdot Z_{чел}(T_{зад}), \quad (В.20)$$

где составные индикаторные коэффициенты определены в В.2.5.3—В.2.5.9.

Если все условия по обеспечению качества используемой информации в допустимых пределах выполнены (т. е. все индикаторные коэффициенты $Z = 1$), риск нарушения надежности реализации процесса функционирования системы по варианту 2, совпадающий с риском нарушения качества используемой информации в процессе функционирования $Z_{\text{обобщен -2}}(T_{\text{зад}})$ полагают несущественным, т. е. формально этим риском можно пренебречь и приравнять нулю. Это означает, что все составные риски нарушения качества используемой информации не превышают допустимого уровня. Для случая обобщенного риска, отличного от нуля, использование коэффициентов, ориентированных на выполнение задаваемых условий α, позволяет осуществлять системный анализ лишь наиболее чувствительных свойств моделируемой системы, которые приводят к возникновению недопустимых рисков при невыполнении или игнорировании задания этих условий.

В.2.5.11 В системном анализе процесса функционирования системы модели В.2.5.3—В.2.5.10 применимы для прогнозирования рисков по варианту 2 выполнения функций, когда результат выполнения функции определяется надежностью и своевременностью представления, полнотой и достоверностью информации и безошибочностью действий должностных лиц.

Детальный учет особенностей процесса функционирования системы по варианту 2 выполнения функций осуществляют на уровне соответствующих методик системного анализа (см. приложение Е).

В.2.6 Расчет обобщенного риска для варианта 3 выполнения функций (при комбинации вариантов 1, 2)

В.2.6.1 Для варианта 3 (см. В.2.1) результат выполнения функций без учета требований по защите информации зависит как от случайных событий, связанных с возникновением технических отказов (по варианту 1), так и от качества используемой информации (по варианту 2). Показатель обобщенного риска нарушения надежности реализации процесса функционирования системы по варианту 3 выполнения функций в этом случае учитывает результаты моделирования согласно В.2.2 — В.2.4 по варианту 1 и В.2.5 по варианту 2. Обобщенный риск для варианта 3 используют для сравнения весомости прогнозируемых частных рисков, выявления явных и скрытых угроз и поддержки принятия решений для задач системного анализа согласно разделу 7 и ГОСТ Р 59349.

В.2.6.2 В сопоставлении с возможным ущербом обобщенный риск нарушения надежности реализации процесса функционирования системы $Z_{\text{обобщен -3}}(T_{\text{зад}})$ по варианту 3 выполнения функций без учета требований по защите информации для периода прогноза $T_{\text{зад}}$ определяют по формуле

$$Z_{\text{обобщен -3}}(T_{\text{зад}}) = 1 - Z_{\text{надежн -1}}(T_{\text{зад}}) \cdot Z_{\text{над предст}}(T_{\text{зад}}) \cdot Z_{\text{своевр}} \cdot Z_{\text{полн}} \cdot Z_{\text{акт}} \cdot Z_{\text{безош}} \cdot Z_{\text{корр}} \cdot Z_{\text{чел}}(T_{\text{зад}}), \qquad \text{(В.21)}$$

где $Z_{\text{надежн -1}}(T_{\text{зад}})$ — коэффициент надежности реализации процесса в системе по варианту 1 (см. В.2.4.5),

$Z_{\text{над предст}}(T_{\text{зад}})$, $Z_{\text{своевр}}$, $Z_{\text{полн}}$, $Z_{\text{акт}}$, $Z_{\text{безош}}$, $Z_{\text{корр}}$, $Z_{\text{чел}}(T_{\text{зад}})$ — составные коэффициенты для расчетов по варианту 2 (см. В.2.5.3—В.2.5.9).

В.2.6.3 Если для расчетов по формуле (В.21) все условия α выполнены (т. е. все коэффициенты $Z = 1$), обобщенный риск нарушения надежности реализации процесса функционирования системы $Z_{\text{обобщен -3}}(T_{\text{зад}})$ полагают несущественным, риск формально приравнивают к нулю. Это означает, что все составные риски не превышают допустимого уровня. Для случая обобщенного риска, отличного от нуля, использование индикаторных коэффициентов, ориентированных на выполнение задаваемых условий α, позволяет осуществлять системный анализ лишь наиболее чувствительных свойств системы, которые приводят к возникновению недопустимых рисков при невыполнении или игнорировании задания этих условий.

Детальный учет особенностей процесса функционирования системы по варианту 3 выполнения функций осуществляют на уровне соответствующих методик системного анализа (см. приложение Е).

В.3 Математические модели для прогнозирования риска нарушения требований по защите информации

В.3.1 Общие положения

Прогнозирование рисков нарушения требований по защите информации осуществляют на основе применения математических моделей для прогнозирования риска нарушения требований по защите информации ГОСТ Р 59341—2021 (В.2 приложения В). Все положения по моделированию, изложенные в ГОСТ Р 59341 для процесса управления информацией, в полной мере применимы для прогнозирования риска нарушения требований по защите информации в процессе функционирования системы (в части, свойственной этому процессу и выполняемым функциям).

В моделях простой структуры под анализируемой системой понимается определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявляют требования и применяют меры защиты информации. Такую систему рассматривают как «черный ящик», если для него сделано предположение об использовании одной и той же модели угроз безопасности информации, и одной и той же технологии системного контроля выполнения требований по защите информации и восстановления системы после состоявшихся нарушений или выявленных предпосылок к нарушениям. В моделях сложной структуры под анализируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логи-

чески представляет собой выходной результат и совокупность задействованных активов (выходной результат становится активом в итоге выполняемых действий), к которым предъявляют требования и применяют меры защиты информации. В общем случае для системы сложной структуры для различных элементов могут быть применены различные модели угроз безопасности информации или различные технологии системного контроля выполнения требований по защите информации и восстановления системы. Отдельный элемент рассматривается как «черный ящик».

Под целостностью моделируемой системы понимается такое ее состояние, которое в течение задаваемого периода прогноза отвечает целевому назначению модели системы. При моделировании, направленном на прогнозирование риска нарушения требований по защите информации, целевое назначение моделируемой системы проявляется в выполнении требований по защите информации. В этом случае для каждого из элементов и моделируемой системы в целом пространство элементарных состояний на временной оси образуют два основных состояния:

- «Выполнение требований по защите информации в системе обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации;
- «Выполнение требований по защите информации в системе нарушено» — в противном случае.

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

Аналогично В.2 применяют математическую модель «черного ящика» при отсутствии какого-либо контроля или математическую модель «черного ящика» при реализации технологии периодического системного контроля, каждая из которых адаптирована к контексту защиты информации — см. ГОСТ Р 59341—2021, В.2 приложения В.

С формальной точки зрения при сопоставлении с возможным ущербом модель позволяет оценить вероятностное значение риска нарушения требований по защите информации в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения требований по защите информации в процессе функционирования системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики). При этом учитываются предпринимаемые меры периодической диагностики и восстановления возможностей по обеспечению выполнения требований по защите информации.

В.3.2 Исходные данные и расчетные показатели

Для расчета вероятностных показателей применительно к моделируемой системе, где анализируемые сущности (выходные результаты, действия) могут быть представлены в виде системы или системного элемента — «черного ящика», используют исходные данные, формально определяемые в общем случае следующим образом:

σ — частота возникновения источников угроз нарушения требований по защите информации в процессе функционирования системы;

β — среднее время развития угроз с момента возникновения источников угроз до нарушения нормальных условий функционирования системы (например, до нарушения установленных требований по защите информации в системе или до инцидента);

$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей по выполнения требований по защите информации в системе;

$T_{диаг}$ — среднее время системной диагностики возможностей по обеспечению выполнения требований по защите информации (т. е. диагностики целостности моделируемой системы);

$T_{восст}$ — среднее время восстановления нарушенных возможностей по обеспечению выполнения требований по защите информации в моделируемой системе;

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

Расчетные показатели:

$P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ — вероятность отсутствия нарушения требований защите информации в моделируемой системе в течение периода $T_{зад}$;

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

Расчет показателей применительно к процессу определения архитектуры для моделируемой системы простой или сложной структуры осуществляют по формулам ГОСТ Р 59341—2021 (В.2 приложения В). Расчет вероятности нарушения требований по защите информации в системе для процесса определения архитектуры системы в течение периода прогноза $R_{наруш}(T_{зад}) = R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ осуществляют как дополнение до единицы значения $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$.

Примечание — При необходимости могут быть использованы адаптированные модели, позволяющие оценивать защищенность от опасных программно-технических воздействий, от несанкционированного доступа и сохранение конфиденциальности информации в системе — см. ГОСТ Р 59341—2021 (В.3 приложения В).

В.4 Прогнозирование интегрального риска нарушения реализации процесса с учетом требований по защите информации

При расчетах интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации используют результаты расчетов обобщенного риска нарушения надежности реализации процесса без учета требований по защите информации (по моделям и методам В.2) и риска нарушения требований по защите информации (по рекомендациям В.3). При этом для оценки обобщенного риска $Z_{\text{обобщен}}(T_{\text{зад}})$ нарушения надежности реализации процесса функционирования системы без учета требований по защите информации в течение периода прогноза $T_{\text{зад}}$ учитывают возможные варианты 1, 2, 3 выполнения функций (см. В.2.1)

$$Z_{\text{обобщен}}(T_{\text{зад}}) = \begin{cases} Z_{\text{обобщен-1}}(T_{\text{зад}}) \text{ для варианта 1 выполнения функций, расчет по (В.12);} \\ Z_{\text{обобщен-2}}(T_{\text{зад}}) \text{ для варианта 2 выполнения функций, расчет по (В.20);} \\ Z_{\text{обобщен-3}}(T_{\text{зад}}) \text{ для варианта 3 выполнения функций, расчет по (В.21).} \end{cases} \quad \text{(В.22)}$$

В сопоставлении с возможным ущербом интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$ для периода прогноза $T_{\text{зад}}$ определяют по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - [1 - Z_{\text{обобщен}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})], \quad \text{(В.23)}$$

где $R_{\text{наруш}}(T_{\text{зад}})$ — вероятность нарушения требований по защите информации в системе для процесса функционирования системы в течение периода прогноза $T_{\text{зад}}$, рассчитывается по рекомендациям В.3.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса функционирования системы

Г.1 Общие положения

Г.1.1 Настоящие методические указания определяют типовые действия при расчетах основных количественных показателей рисков в процессе функционирования системы:

- риска нарушения надежности реализации процесса функционирования системы без учета требований по защите информации;
- риска нарушения требований по защите информации в процессе функционирования системы;
- интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации.

При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможным ущербом.

Примечание — Для разработки самостоятельной методики по оценке ущербов согласно приложению Е учитывают специфику систем (см., например, ГОСТ Р 22.10.01, ГОСТ Р 54145).

Г.1.2 Прогнозирование рисков осуществляют с использованием формализованного представления реальной системы в виде моделируемой системы.

Г.1.3 Применительно к конкретной системе в целях прогнозирования рисков определению подлежат:

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

Г.1.4 В качестве мер противодействия угрозам, способных при их применении снизить расчетные риски, могут выступать более частая (по сравнению со временем развития угроз) системная диагностика или контроль с восстановлением нормального функционирования моделируемой системы.

Г.1.5 Обоснованное определение сбалансированных системных мер, предупреждающих возникновение ущербов при ограничениях на ресурсы и допустимые риски, а также оценка и обоснование эффективных кратко-, средне- и долгосрочных планов по обеспечению безопасности осуществляют путем решения самостоятельных оптимизационных задач, использующих расчетные значения прогнозируемых рисков (см. рекомендуемый перечень методик в приложении Е).

Примечание — Рекомендации по задачам системного анализа приведены в ГОСТ Р 59349.

Г.1.6 По мере решения на практике задач анализа и оптимизации для различных объектов и логических структур моделируемой системы создают базы знаний, содержащие варианты решения типовых задач сбалансированного управления рисками.

Примечание — Примерами практического применения общих методических положений к системам дистанционного контроля в опасном производстве могут служить положения ГОСТ Р 58494—2019 (приложения А—Е).

Г.2 Цель прогнозирования рисков

Основной целью прогнозирования рисков является установление степени вероятного нарушения требований по защите информации и/или нарушения надежности реализации исследуемого процесса функционирования системы с учетом требований по защите информации за заданный период прогноза. Прогнозирование рисков осуществляют в интересах решения определенных задач системного анализа (см. раздел 7). Конкретные практические цели прогнозирования рисков устанавливают заказчик системного анализа и/или аналитик моделируемой системы при выполнении работ системной инженерии.

Г.3 Положения формализации

Г.3.1 Для решения задач системного анализа в качестве моделируемой системы могут выступать: множество выходных результатов, множество действий рассматриваемого процесса или иные сущности, объединенные целевым назначением при моделировании.

Г.3.2 Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи системного анализа. В общем случае моделируемую систему представляют либо в виде «черного ящика» (см. В.2.1 и В.2.2), либо в виде сложной структуры, элементы которой соединяются последовательно или параллельно (см. В.2.3).

Для получения более точных результатов прогнозирования рисков осуществляют декомпозицию сложной моделируемой системы до уровня составных системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых для описания целостности моделируемой системы логическими условиями «И» и «ИЛИ».

Примечания

1 Логическое условие «И» для двух связанных этим условием элементов интерпретируется так: моделируемая система из двух последовательно соединяемых элементов находится в состоянии целостности, когда первый элемент «И» второй элемент находятся в состоянии целостности.

2 Логическое условие «ИЛИ» для двух связанных этим условием элементов интерпретируется так: система из двух параллельно соединяемых элементов находится в состоянии целостности, когда первый элемент «ИЛИ» второй элемент находятся в состоянии целостности (в частности, когда для повышения надежности дублируется выполнение отдельных действий).

Для каждого из элементов, а также для моделируемой системы в целом вводится пространство элементарных состояний (с учетом логических взаимосвязей элементов условиями «И», «ИЛИ»).

Г.3.3 В приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси могут быть формально определены двумя основными состояниями:

- «Выполнение требований по защите информации в процессе функционирования системы обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации, т. е. с точки зрения математического моделирования их невыполнение недопустимо;
- «Выполнение требований по защите информации в процессе функционирования системы нарушено» — в противном случае.

Г.3.4 В приложении к прогнозированию интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации пространство элементарных состояний на временной оси могут быть формально определены другими двумя основными состояниями:

- «Надежность реализации процесса функционирования системы «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены «И» надежность выполнения определенных действий процесса для получения выходных результатов, «И» выполнение определенных требований по защите информации;
- «Надежность реализации процесса функционирования системы «И»/«ИЛИ» выполнение требований по защите информации в системе нарушены» — в противном случае.

Г.3.5 В общем случае с применением 1-го способа по В.2.4 возможно расширение или переименование самих элементарных состояний, главное, чтобы они формировали полное множество аналогично множествам, введенным в Г.3.3, Г.3.4.

Г.4 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе, которая может быть представлена в виде «черного ящика» (см. В.2.1, В.2.2, В.2.5) или сложной логической структуры (см. В.2.3, В.2.4, В.2.6, В.3, В.4), основными расчетными показателями являются:

$R_{\text{надежн}}(T_{\text{зад}})$ — риск нарушения надежности реализации процесса функционирования системы без учета требований по защите информации в течение задаваемого периода прогноза;

$R_{\text{наруш}}(T_{\text{зад}})$ — риск нарушения требований по защите информации в процессе функционирования системы в течение задаваемого периода прогноза;

$R_{\text{интегр}}(T_{\text{зад}})$ — интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации в течение задаваемого периода прогноза.

Применительно к моделируемой системе исходными данными являются исходные данные, необходимые для проведения расчетов по моделям подразделов В.2 и В.3. Расчеты осуществляют по рекомендациям В.2—В.4.

Примечание — Согласно В.1 рекомендации разделов В.2—В.4 приведены в приложении к отдельной функции или объединенному множеству функций без их дифференциации по отдельным функциям. При необходимости детального учета каждой из M функций, реализуемых системой ($m = 1,\ldots,M$), все положения В.2—В.4 могут быть применены к каждой m-й функции отдельно. Тогда в приложении к каждой m-й функции может быть определен свой интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации в течение задаваемого периода прогноза $R_{\text{интегр }m}(T_{\text{зад}})$. В этом случае по всем M функциям в предположении независимости их выполнения интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации в течение задаваемого периода прогноза $T_{\text{зад}}$ вычисляют по формуле

$$R_{\text{система}}(T_{\text{под}}) = 1 - \prod_{m=1}^{M}[1 - R_{\text{система } m}(T_{\text{под}})]. \quad (Г.1)$$

При этом для всего множества функций применима интерпретация: реализация процесса функционирования системы с учетом требований по защите информации в течение задаваемого периода прогноза будет нарушена, если в течение этого периода она будет нарушена хотя бы в отношении одной из M выполняемых системой функций.

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

Шаг 1. Устанавливают анализируемые объекты и определяют моделируемые системы для прогнозирования рисков. Действия осуществляют согласно Г.1.

Шаг 2. Устанавливают конкретные цели прогнозирования. Действия осуществляют согласно Г.2.

Шаг 3. Выявляют перечень существенных угроз, критичных с точки зрения недопустимого потенциального ущерба (см. также ГОСТ Р 59346, ГОСТ Р 59349). Принимают решение о представлении моделируемой системы в виде «черного ящика» или в виде сложной структуры, декомпозируемой до составных элементов. Формируют пространство элементарных состояний для каждого элемента и моделируемой системы в целом. Действия осуществляют согласно Г.3.

Шаг 4. Выбирают расчетные показатели (см. Г.4). Выбирают подходящие математические модели и методы повышения их адекватности по В.2, В.3, В.4, Г.4. Разрабатывают необходимые методики системного анализа (см. приложение Е). Осуществляют расчет выбранных показателей с использованием расчетных соотношений (В.2)—(В.23), (Г.1).

Шаг 5. Осуществляют действия системного анализа согласно рекомендациям раздела 7 и ГОСТ Р 59349.

Г.6 Обработка и использование результатов прогнозирования

Результаты прогнозирования рисков должны быть удобны для обработки заказчиком системного анализа 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. Результаты расчетов подлежат использованию для решения задач системного анализа — см. раздел 7, приложение Е и ГОСТ Р 59349.

Примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, 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.

Г.7 Материально-техническое обеспечение

В состав материально-технического обеспечения для прогнозирования рисков входят (в части, свойственной процессу функционирования 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 и принимаемых решений).

Г.8 Отчетность

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

Приложение Д
(справочное)

Типовые допустимые значения показателей рисков для процесса функционирования системы

С точки зрения остаточного риска, характеризующего приемлемый уровень целостности систем, 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 функционирования системы, 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 системы.

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

Типовые допустимые значения показателей рисков для процесса функционирования 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 процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Пример задания допустимых значений рисков

Показатель	Допустимое значение риска (в вероятностном выражении)	
	при ориентации на обоснование по прецедентному принципу	при ориентации на обоснование для системы-эталона
Риск нарушения требований по защите информации в процессе функционирования системы	Не выше 0,05	Не выше 0,01
Интегральный риск нарушения реализации процесса функционирования системы с учетом требований по защите информации	Не выше 0,05	Не выше 0,01

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса функционирования системы

Е.1 Методика прогнозирования риска нарушения требований по защите информации в процессе функционирования системы.

Е.2 Методика прогнозирования интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации.

Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации).

Е.4 Методики выявления явных и скрытых недостатков процесса функционирования системы с использованием прогнозирования рисков.

Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса функционирования системы и противодействие угрозам нарушения требований по защите информации.

Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам функционирования системы.

Е.7 Методики инструментально-расчетной оценки показателей устойчивости функционирования системы в условиях информационно-технических воздействий.

Е.8 Методики обоснования способов повышения устойчивости функционирования системы в условиях информационно-технических воздействий.

Примечания

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

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

Библиография

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

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

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

[4] Федеральный закон от 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] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной 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 функционирования системы, риск, система, системная инженерия, управление

Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 11.05.2021. Подписано в печать 20.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,18.

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.
www.gostinfo.ru info@gostinfo.ru