ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59356— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ СОПРОВОЖДЕНИЯ 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 бюджетным учреждением «Научно-технический центр «Энергобезопасность» (ФБУ «НТЦ Энергобезопасность») и Обществом с ограниченной ответственностью «Научно-исследовательский институт прикладной математики и сертификации» (ООО НИИПМС)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 мая 2021 г. № 374-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, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59357. Для процесса сопровождения системы — по настоящему стандарту.

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ СОПРОВОЖДЕНИЯ СИСТЕМЫ

System engineering. Protection of information in system maintenance process

Дата введения — 2021—11—30

1 Область применения

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

Для практического применения в приложениях А—Е приведены примеры перечней активов, подлежащих защите, и угроз, типовые 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 эксплуатации систем и реализующими процесс их сопровождения, 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 15.601 Система разработки и постановки продукции на производство. Техническое обслуживание и ремонт техники. Основные положения

ГОСТ 27.002 Надежность в технике. Термины и определения

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

Издание официальное

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

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

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

ГОСТ 33981 Оценка соответствия. Исследование проекта продукции

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

ГОСТ Р 22.1.12 Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования

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 14764 Информационная технология. Сопровождение программных средств

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

ГОСТ Р ИСО/МЭК 15026-1 Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 1. Понятия и словарь

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

ГОСТ Р 51901.12 (МЭК 60812:2006) Менеджмент риска. Метод анализа видов и последствий отказов

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 55234.3 Практические аспекты менеджмента риска. Процедуры проверки и технического обслуживания оборудования на основе риска

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 57329/EN 13306:2010 Системы промышленной автоматизации и интеграция. Системы технического обслуживания и ремонта. Термины и определения

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—2019 Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 58811 Центры обработки данных. Инженерная инфраструктура. Стадии создания

ГОСТ Р 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 59355 Системная инженерия. Защита информации в процессе функционирования 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

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 57329, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 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, статья 2.3]

3.1.2

адаптивное сопровождение: Изменение (модификация) программного продукта после поставки, обеспечивающее его работоспособность в измененных или изменяющихся условиях (среде).

Примечание — Адаптивное сопровождение обеспечивает модернизацию, позволяющую вносить изменения в эксплуатационную среду программного средства. Данные изменения должны быть внесены для сохранения работоспособности продукта в изменяемой среде. Например, операционная система может быть модернизирована и некоторые изменения должны быть внесены в продукт для его адаптации к новой операционной системе.

[ГОСТ Р ИСО/МЭК 14764—2002, пункт 4.1]

3.1.3

анализ отказов: Логическое и систематическое исследование отказавшего элемента с целью идентификации и анализа характера возникновения отказов, их причин и последствий.

Примечание — Анализ отказов, как правило, проводят для повышения эксплуатационной надежности.

[ГОСТ Р 57329—2016, статья 10.3]

3.1.4

восстановление: Мероприятие после разборки элемента и ремонта/замены субэлементов, срок службы которых подходит к концу и/или которые следует регулярно заменять.

Примечание 1 — Восстановление отличается от капитального ремонта тем, что эта операция может включать в себя модификацию и/или усовершенствование элемента.

Примечание 2 — Целью восстановления элемента, как правило, является увеличение срока его службы.

[ГОСТ Р 57329—2016, статья 8.14]

3.1.5

документация по техническому обслуживанию и ремонту: Часть эксплуатационной документации, которая содержит хронологию поступления всех данных, связанных с техническим обслуживанием и ремонтом элементов.

Примечание — Хронология может содержать записи всех неисправностей, сбоев, затрат, наличия элементов, времени работоспособности и любых других важных данных.

[ГОСТ Р 57329—2016, статья 10.5]

3.1.6

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.7

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]

3.1.8

запасная часть: Отдельная деталь или сборочная единица, предназначенные для замены изношенных, неисправных или отказавших аналогичных частей объекта с целью поддержания или восстановления его работоспособного состояния.

[ГОСТ 18322—2016, статья 2.1.17]

3.1.9

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]

3.1.10

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.11

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]

3.1.12

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]

3.1.13 **интегральный риск нарушения реализации процесса сопровождения 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.

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

3.1.15

интегрированная логистическая поддержка (процессов технической эксплуатации изделия): Совокупность видов деятельности, осуществляемых головным разработчиком изделия совместно с другими участниками жизненного цикла изделия и направленных на формирование системы технической эксплуатации изделия, обеспечивающей эффективное использование изделия при приемлемой стоимости его жизненного цикла.

[ГОСТ Р 53394—2017, статья 3.8]

3.1.16

комплект ЗИП: Набор запасных частей, инструментов, принадлежностей (ЗИП) и расходных материалов, необходимых для функционирования, технического обслуживания и ремонта объекта, скомплектованный в зависимости от назначения и особенностей использования.

Примечание — Комплект ЗИП может рассматриваться как предмет поставки и как набор, формируемый эксплуатирующей организацией. В первом случае комплект ЗИП определяется документацией на объект с учетом назначения и особенностей его использования и входит в комплект поставки на заданный гарантийный срок, во втором — формируется эксплуатирующей организацией с учетом принятого эшелона ТО (ремонта).

[ГОСТ 18322—2016, статья 2.1.19]

3.1.17

корректирующее техническое обслуживание: Техническое обслуживание, выполняемое после обнаружения неисправности с целью возвращения объекта в работоспособное состояние.

[ГОСТ 18322—2016, статья 2.2.21]

3.1.18

материально-техническое обеспечение: Совокупность процедур и методов, направленных на обеспечение своевременных поставок необходимого количества предметов снабжения для производства, применения по назначению и технической эксплуатации изделия и на обеспечение хранения, распределения, пополнения запасов указанных предметов снабжения в течение всего жизненного цикла изделия.

[ГОСТ Р 53394—2017, статья 3.42]

3.1.19 **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.

3.1.20

модификация: Совокупность всех технических, организационных и управленческих мероприятий, направленных на изменение одной или нескольких функций элемента.

Примечание 1 — Модификация не связана с техническим обслуживанием и ремонтом, однако имеет дело с изменением какой-либо функции элемента для получения новой функции. Эти изменения могут оказывать влияние на функциональную надежность элемента.

Примечание 2 — Модификация может включать в себя организацию процедуры технического обслуживания и ремонта.

Примечание 3 — Изменение исходного элемента без изменения его требуемой функции или повышения функциональной надежности называется «заменой» и не является модификацией.

[ГОСТ Р 57329—2016, статья 8.13]

3.1.21

мониторинг (контроль) текущего состояния: Мероприятие, осуществляемое либо вручную, либо автоматически, и предназначенное для измерения характеристик и параметров фактического состояния элемента через заданные интервалы времени.

Примечание 1 — Мониторинг отличается от осмотра тем, что его используют для оценки любых изменений параметров элемента в течение времени.

Примечание 2 — Мониторинг может быть непрерывным, в течение определенного времени или после заданного числа операций.

Примечание 3 — Мониторинг обычно осуществляется в рабочем состоянии элемента.

[ГОСТ Р 57329—2016, статья 8.2]

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

3.1.23

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.24

периодическое техническое обслуживание: Плановое техническое обслуживание, выполняемое через установленные в документации значения наработки или интервалы времени.

[ГОСТ 18322—2016, статья 2.2.14]

3.1.25

план сопровождения: Документ, излагающий соответствующие методы сопровождения, описывающий необходимые ресурсы и работы применительно к сопровождению программного продукта.

Примечание — План сопровождения готовит соответствующая организация (персонал сопровождения, сопроводитель). Данный план должен быть реализован сразу после передачи продукта на сопровождение.

[ГОСТ Р ИСО/МЭК 14764—2002, пункт 4.6]

3.1.26

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.27

поставщик: Организация или лицо, которые вступают в соглашение с приобретающей стороной на поставку продукта или услуги.

Примечание 1 — Поставщиком может быть подрядчик, производитель, торговец или продавец.

Примечание 2 — Иногда приобретающая сторона и поставщик являются частью одной и той же организации.

[ГОСТ Р 57193—2016, пункт 4.1.43]

3.1.28

предупредительное техническое обслуживание и ремонт, основанные на прогнозировании: Работы, основанные на данных технологии, имеющие целью исключение проблем технического обслуживания и ремонта с использованием прогнозирования вероятных режимов отказов.

[ГОСТ Р 57329—2016, статья 7.4]

3.1.29

профилактическое сопровождение: Модификация программного продукта после поставки в целях обнаружения и корректировки имеющихся в нем скрытых ошибок для предотвращения явного проявления этих ошибок при эксплуатации данного продукта.

[ГОСТ Р ИСО/МЭК 14764—2002, пункт 4.11]

3.1.30

профилактическое техническое обслуживание: Плановое техническое обслуживание, выполняемое через определенные интервалы времени и направленное на поддержание работоспособного состояния объекта, на раннее выявление неисправностей и снижение вероятности отказов.

[ГОСТ 18322—2016, статья 2.2.20]

3.1.31

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

[ГОСТ Р 57329—2016, статья 6.5]

3.1.32

ремонт: Комплекс технологических операций и организационных действий по восстановлению работоспособности, исправности и ресурса объекта и/или его составных частей.

Примечание — Ремонт включает операции локализации, диагностирования, устранения неисправности и контроль функционирования.

[ГОСТ 18322—2016, статья 2.1.2]

3.1.33

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.34

сбой, неисправность: Состояние элемента, характеризующееся неспособностью выполнить требуемую функцию, исключая такую неспособность во время профилактического технического обслуживания и ремонта или других запланированных действий или из-за нехватки внешних ресурсов.

Примечание — При выявлении дефектов, в результате сбоя, как правило, возникает отказ, однако в некоторых случаях может возникать и предварительный сбой.

[ГОСТ Р 57329—2016, статья 6.1]

3.1.35

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 использованием 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]

3.1.36 **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.

3.1.37

системный элемент: Представитель совокупности элементов, образующих систему.

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

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

[ГОСТ Р 57193—2016, пункт 4.1.45]

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

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

3.1.39

техническое обслуживание; ТО: Комплекс технологических операций и организационных действий по поддержанию работоспособности или исправности объекта при использовании по назначению, ожидании, хранении и транспортировании.

[ГОСТ 18322—2016, статья 2.1.1]

3.1.40

техническое обслуживание в особых условиях: Техническое обслуживание, выполняемое в особых условиях эксплуатации объекта, указанных в отраслевой документации и характеризуемых значениями параметров, выходящими за пределы допустимых границ.

Примечание — Особые условия могут быть природного, техногенного характера и др.

[ГОСТ 18322—2016, статья 2.2.7]

3.1.41

техническое обслуживание и ремонт по состоянию: Профилактическое техническое обслуживание и ремонт, основанные на оценке результатов мониторинга физических параметров.

Примечание — Мониторинг состояния, и/или проверки, и/или испытания могут быть плановыми, по запросу или непрерывными.

[ГОСТ Р 57329—2016, статья 7.3]

3.1.42

техническое обслуживание, обеспечивающее надежность: Техническое обслуживание, предусматривающее выполнение только тех работ, которые направлены на предупреждение, выявление и устранение конкретных влияющих на уровень надежности и безопасности изделия видов его отказов.

Примечание — Обоснование состава и периодичности указанных работ по техническому обслуживанию выполняют путем проведения специального анализа видов и последствий возможных отказов изделия и его составных частей.

[ГОСТ Р 53394—2017, статья 3.35]

3.1.43

техническое обслуживание с непрерывным контролем: Техническое обслуживание, предусмотренное документацией и выполняемое по результатам непрерывного контроля технического состояния объекта.

[ГОСТ 18322—2016, статья 2.2.18]

3.1.44

техническое обслуживание с периодическим контролем: Техническое обслуживание, выполняемое при контроле технического состояния объекта в объеме и с периодичностью, установленными в документации, при этом объем остальных операций определяется техническим состоянием объекта в момент начала технического обслуживания.

[ГОСТ 18322—2016, статья 2.2.17]

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

3.1.46

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использованы следующие сокращения:

ЗИП — запасные части, инструменты, принадлежности;

СМИК — система мониторинга инженерных (несущих) конструкций, опасных природных процессов и явлений;

СМИС — система мониторинга и управления инженерными системами;

ССП — система сбора данных и передачи сообщений;

СУКС — система связи и управления в кризисных ситуациях;

ТЗ — техническое задание;

ТО — техническое обслуживание.

4 Основные положения системной инженерии по защите информации в процессе сопровождения системы

4.1 Общие положения

Организации используют процесс сопровождения системы для поддержки работоспособности, устранения неисправностей, обеспечения и/или повышения безопасности, качества и эффективности системы при ее эксплуатации. В процессе сопровождения 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 сопровождения системы и обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах используют системный анализ процесса с учетом требований по защите информации.

Определение выходных результатов процесса сопровождения системы и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 15.601, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 14764, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58811. 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 55234.3, ГОСТ Р 57272.1, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59355 с учетом специфики сопровождаемой системы (см., например, [21]—[26]).

4.2 Цели процесса и назначение мер защиты информации

4.2.1 Определение целей процесса сопровождения системы осуществляют с использованием ГОСТ 15.601, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 14764, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58811 с учетом специфики сопровождаемой системы.

В общем случае главной целью процесса сопровождения системы является поддержание функционирования системы в соответствии с ее назначением и предъявляемыми системными требованиями. В рамках процесса выполняют:

- мониторинг или периодический контроль текущего состояния системы и ее возможностей, обеспечивающих удовлетворение требований заинтересованных сторон;
- контроль выполнения предъявляемых к системе эксплуатационных требований;
- необходимые действия корректирующего ТО и адаптивного сопровождения системы (направленные на упреждение возникновения и ликвидацию последствий возможных сбоев, отказов и инцидентов, а также на совершенствование информационного, математического, методического, метрологического, организационного, программного, технического и иных видов обеспечения системы), иные различные виды ТО (в т. ч. ТО и ремонт по состоянию, ТО, обеспечивающее надежность, ТО с периодическим и непрерывным контролем, ТО в особых условиях эксплуатации);
- сопровождение программных средств и систем;
- регистрацию и анализ сбоев, отказов и инцидентов, возникающих в ходе эксплуатации системы;
- подтверждение работоспособного состояния системы по результатам устранения последствий сбоев, отказов и инцидентов.

4.2.2 Меры защиты информации в процессе сопровождения системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, а также для предотвращения утечки защищаемой информации, 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 50922, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [20]—[24] с учетом специфики сопровождаемой системы.

4.3 Место процесса сопровождения в жизненном цикле системы

Процесс сопровождения системы выполняется на стадии эксплуатации системы. Процесс опирается на результаты предшествующих стадий создания, модернизации или развития системы. Перечень конкретных работ при сопровождении системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р 51583, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58811. Процесс сопровождения системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы и, при необходимости, включать в себя другие процессы.

4.4 Основные принципы системного анализа

При проведении системного анализа процесса сопровождения 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, [20]—[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 по обеспечению защиты информации в процессе сопровождения 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 сопровождения системы

5.1 Общие требования системной инженерии по защите информации в процессе сопровождения системы устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения детализируют в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например, [1]—[26]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

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 сопровождения системы и поддержке при этом эффективности защиты информации.

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

- требования к составам выходных результатов процесса, выполняемых действий и используемых при этом активов, требующих защиты информации;
- требования к определению потенциальных угроз и возможным сценариям возникновения и развития угроз для выходных результатов и выполняемых действий процесса;
- требования к прогнозированию рисков, обоснованию эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

5.3 Состав выходных результатов и выполняемых действий в процессе сопровождения системы определяют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.601, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 14764, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58811 с учетом специфики сопровождаемой системы.

Примечание — В процессе сопровождения 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 сопровождения 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, привлекаемых информационных систем и/или баз 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 15.601, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО/МЭК 14764, 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 IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 20000-1, 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]—[26].

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

5.6 Эффективность защиты информации при выполнении процесса сопровождения 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 сопровождения системы осуществляют с использованием методов, моделей и методических указаний, представленных в приложениях В, Г, Д с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 55234.3, 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 сопровождения системы определен в 6.3.

Типовые модели и методы прогнозирования рисков в процессе сопровождения 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 и действий защиты информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам и возможным условиям 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 сопровождения системы, к которым предъявлены 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 сопровождения системы являются:

- стратегия сопровождения системы, которая определяет методы управления, сроки, ресурсы и условия, необходимые для достижения целей сопровождения, включая:
- планы упреждающих действий, направленных на минимизацию риска нарушения безопасности, качества, эффективности функционирования системы,
- стратегию материально-технического обеспечения и интегрированной логистической поддержки процесса, предусматривающую доступность необходимых ресурсов и материалов,
- меры противодействия поступлению контрафактных системных элементов,
- требования к кадрам,
- набор показателей, необходимых для проведения оценки безопасности, качества и эффективности функционирования системы, а также результативности процесса сопровождения системы;
- планы по обеспечению замены хранимых системных элементов, запасных частей (комплектов ЗИП), местоположению, условиям их хранения и расходным нормам замены, результаты реализации этих планов;

- планы по сопровождению системы, материально-техническому обеспечению и поддержке жизненного цикла системы, результаты реализации этих планов;
- ограничения в применении системы, вытекающие из потребностей ее сопровождения;
- доступ к обеспечивающим системам и системным элементам, услугам и материалам, необходимым для сопровождения системы;
- отчеты о проведении обучения операторов, пользователей и других заинтересованных сторон, задействованных для применения и поддержания эксплуатации системы после действий по ее сопровождению;
- отчеты о результатах сопровождения системы, включающие документацию по сопровождению, оценку степени достижения цели процесса сопровождения, результаты анализа возникающих инцидентов, сбоев и отказов, предложения по модификации, модернизации, совершенствованию или развитию системы (при их наличии), сведения о предполагаемых затратах, необходимых для дальнейшего сопровождения системы;
- карту прослеживаемости между действиями по сопровождению системы, системными элементами и артефактами системы.

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

- подготовительные мероприятия:
- определение стратегии сопровождения системы, включая виды проводимых мероприятий ТО, например, ТО и ремонт по состоянию, ТО, обеспечивающее надежность, ТО с периодическим и непрерывным контролем, ТО в особых условиях эксплуатации (по ГОСТ Р ИСО/МЭК 14764, ГОСТ Р 51901.12, ГОСТ Р 55234.3),
- подготовку планов сопровождения, материально-технического обеспечения и поддержания жизненного цикла системы,
- определение ограничений системы, следующих из потребностей ее сопровождения,
- получение или приобретение доступа к обеспечивающим системам и системным элементам, необходимым по жизненному циклу системы, к запасным частям, услугам и материалам, предполагаемым к использованию в процессе сопровождения системы;
- выполнение необходимых действий по сопровождению системы, включая:
- регистрацию и анализ возникающих инцидентов, сбоев и отказов с целью устранения негативных последствий, а также их анализ и планирование необходимых упреждающих действий по их предотвращению,
- выполнение регламентных процедур по устранению сбоев и/или замене системных элементов и восстановлению системы до уровня ее эксплуатационного состояния или запасного (резервного) режима эксплуатации,
- выполнение процедур упреждающего сопровождения системы, обеспечивая замену или обслуживание системных элементов согласно плановым срокам (т. е. до наступления отказа),
- идентификацию отказов при выявлении несоответствий в функционировании системы,
- отслеживание моментов, когда требуется модификация (адаптация) или усовершенствование системы,
- приобретение, обучение и аттестацию персонала для обеспечения и поддержания достаточного числа операторов системы (по мере необходимости);
- обеспечение интегрированной логистической поддержки процесса сопровождения системы, включая:
- анализ эффективности по затратам (результаты которого могут повлиять на начальный проект системы или планирование запасных частей и регламентное обслуживание в период эксплуатации, а также потребовать управления цепочками поставок),
- необходимые действия для того, чтобы требуемые ресурсы были доступны в нужном месте и в нужное время,
- комплектование, обработку, хранение и транспортировку системных элементов и запасных частей, необходимых по жизненному циклу системы,
- постоянный контроль за тем, чтобы планируемые действия логистики отвечали требованиям процесса сопровождения системы, были выполнимыми и поддерживались ресурсами, в т. ч. обученным персоналом;
- управление результатами сопровождения системы, включая:

- регистрацию и анализ результатов сопровождения и логистики, отклонений от штатного исполнения, сбоев, отказов, инцидентов и проблем, возникающих во время эксплуатации, выработку мер реакции на отклонения,

- определение тенденций в возникновении сбоев, отказов, инцидентов, проблем и отклонений в действиях логистики и сопровождения,

- поддержку прослеживаемости между действиями по сопровождению системы, системными элементами и артефактами системы,

- обеспечение сохранности и своевременной модификации основных информационных объектов процесса,

- контроль удовлетворенности заинтересованных сторон функционированием и обеспечением сопровождения системы,

- подготовку отчетов о результатах сопровождения системы.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процесса сопровождения 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 обеспечивать проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения реализации процесса сопровождения системы с учетом требований по защите информации.

Эффективность защиты информации оценивают с использованием 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 действия. 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 сопровождения системы используют следующие количественные показатели:

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

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

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

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

6.3.3 Риск нарушения требований по защите информации в процессе сопровождения 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 требования по защите информации.

6.3.4 Интегральный риск нарушения реализации процесса сопровождения 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 сопровождения системы):

- временные данные функционирования системы защиты информации, в том числе срабатывания ее исполнительных механизмов;
- текущие и статистические данные о состоянии параметров системы защиты информации (привязанные ко временам изменения состояний);
- текущие и статистические данные о самой системе или системах-аналогах, в том числе 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 результаты 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 сопровождения системы включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в процессе сопровождения 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 33981, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/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 сопровождаемой системы (см., например, [21]—[26]).

Примечание — Примеры решения задач системного анализа в приложении к процессу сопровождения системы приведены в Приложении Г, а в приложении к другим процессам — 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.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе сопровождения 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 сопровождению системы;
- финансовые и плановые документы, связанные с сопровождением системы;
- документацию при выполнении научно-исследовательских работ (по ГОСТ 7.32, ГОСТ 15.101) с учетом специфики сопровождаемой системы;
- конструкторскую и технологическую документацию (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);
- документацию системы менеджмента качества организации (по ГОСТ Р ИСО 9001);
- технические задания (по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839);
- 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 специфики сопровождаемой системы.

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе сопровождения 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 сопровождения системы (по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124);
- угрозы безопасности информации при подготовке и обработке документов (по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412);
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) [по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010 (приложение С), ГОСТ Р ИСО/МЭК 27036-2];
- угрозы компрометации информационной безопасности приобретающей стороны, угрозы возникновения ущерба репутации и/или потери доверия поставщика к конкретной приобретающей стороне, информация и информационные системы которой были скомпрометированы (по ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, 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, ГОСТ Р 59215);
- угрозы, связанные с нарушением интеллектуальной собственности;
- прочие соответствующие угрозы безопасности информации, связанные с человеческим фактором, 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 Основные положения

В.1.1 Для прогнозирования рисков в процессе сопровождения системы могут применяться любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Типовые модели и методы прогнозирования рисков обеспечивают вероятностную оценку следующих показателей:

- риска нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации (см. В.1.2—В.1.8, В.2);
- риска нарушения требований по защите информации в процессе сопровождения системы (см. В.3);
- интегрального риска нарушения реализации процесса сопровождения системы с учетом требований по защите информации (см. В.4).

В.1.2 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, и данные собираемой и накапливаемой статистики по процессам и возможным условиям их реализации.

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

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

В.1.4 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований 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 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 успешной реализации процессов.

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

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

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

В.1.8 Изложение моделей в В.2 дано в контексте нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации, в В.3 приведены способы прогнозирования риска нарушения требований по защите информации в процессе (в т. ч. с использованием моделей В.2). Методы прогнозирования интегрального риска нарушения реализации процесса сопровождения системы с учетом требований по защите информации представлены в В.4.

В приложении Г изложены методические указания по прогнозированию рисков.

В.1.9 Другие возможные подходы и подходы, подобные изложенным в В.2, В.3, 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 58494, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, 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 для прогнозирования риска нарушения надежности реализации процесса сопровождения системы

В.2.1 Общие положения

В.2.1.1 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 Для каждого элемента моделируемой системы возможны либо отсутствие какого-либо контроля, либо периодический системный контроль (диагностика) его целостности с необходимым восстановлением по результатам контроля.

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

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

Примечание — Например, надежность реализации процесса сопровождения системы в течение задаваемого периода прогноза обеспечена, если в течение этого периода для всех недублируемых элементов моделируемой системы (т. е. для всех сущностей, логически объединяемых условием «И») обеспечена их целостность, т. е. на временной оси наблюдается элементарное состояние «Целостность элемента моделируемой системы сохранена» — см. также В.2.4.

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

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

Моделируемая система представлена в виде «черного ящика», функционирование которого не контролируется. Восстановление возможностей по обеспечению выполнения действий процесса осуществляется 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 сопровождения системы 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 сопровождения 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, используют формулы (В.1)—(В.5).

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

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

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

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

В рамках модели развитие событий в системе считается не нарушающим надежность реализации процесса сопровождения 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 сопровождения системы, но и способы поддержания и/или восстановления возможностей по выполнению процесса при выявлении источников или следов активизации угроз. Восстановление осуществляется лишь в период системного контроля. Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии удержания рисков в допустимых пределах при реализации процесса сопровождения системы в условиях возможных угроз в течение периода прогноза (т. к. 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 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 угрозы 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 им.

Надежность реализации процесса сопровождения системы считается нарушенной лишь после того, как активизация источника угрозы происходит за период прогноза (т. е. возникает элементарное состояние «Целостность элемента моделируемой системы нарушена», означающее реализацию угрозы). При отсутствии нарушений результатом применения очередной системной диагностики является подтверждение возможностей по реализации процесса, а при наличии нарушений — полное восстановление нарушенных возможностей реализации процесса до приемлемого уровня. С точки зрения системной инженерии результатом применения модели является расчетная вероятность нарушения надежности реализации процесса сопровождения системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики) целостности системы.

Для моделируемой системы, представленной в виде «черного ящика», применительно к выполняемым действиям, выходным результатам рассматриваемого процесса и защищаемым активам формально определяют следующие исходные данные:

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

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

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

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

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

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

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

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

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

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

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

Возможны два варианта:

- вариант 1 — заданный оцениваемый период прогноза $T_{\text{зад}}$ меньше периода между окончаниями соседних контролей ($T_{\text{зад}} < T_{\text{меж}} + T_{\text{диаг}}$);
- вариант 2 — заданный оцениваемый период прогноза $T_{\text{зад}}$ больше или равен периоду между окончаниями соседних контролей ($T_{\text{зад}} \geq T_{\text{меж}} + T_{\text{диаг}}$), 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 варианта 1 при условии независимости исходных характеристик вероятность $P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ отсутствия нарушений надежности реализации процесса сопровождения системы в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле

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

Примечание — Формулу (В.2) используют также для оценки риска отсутствия нарушений надежности реализации процесса сопровождения 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 варианта 2 при условии независимости исходных характеристик вероятность отсутствия нарушений надежности реализации процесса сопровождения системы в течение прогноза $T_{\text{зад}}$ вычисляют по формуле

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

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

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

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

$P_{\text{кон}}$ — вероятность отсутствия нарушений надежности реализации процесса сопровождения системы после последнего системного контроля, вычисляемая по формуле (В.2), т. е.

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

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

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

Формула (В.3) 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 $T_{\text{зад}}$.

Примечание — Для расчетов $P_{\text{возд}(2)}$ 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 сопровождения системы в течение периода прогноза $T_{\text{зад}}$ определяется аналитическими выражениями (В.2)—(В.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (В.1) вероятность нарушения надежности реализации процесса сопровождения системы $R_{\text{надежн}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ в течение заданного пе-

риода 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 сопровождения системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

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

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

Описанные в В.2.2 и В.2.3 модели применимы для проведения оценок, когда 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 создание моделей для систем сложной структуры и более общего случая, когда значения времен системной диагностики и восстановления нарушенных возможностей системы различны.

Расчет основан на применении следующих инженерных способов.

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

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», то в контексте надежности реализации процесса это интерпретируется так: «в системе обеспечена надежности реализации процесса в течение времени t, если 1-й элемент «И» 2-й элемент сохраняют свои возможности по надежной реализации процесса в течение этого времени». Если два элемента соединяются параллельно, что означает логическое соединение «ИЛИ», это интерпретируется так: «система сохраняет возможности по надежной реализации процесса в течение времени t, если 1-й элемент «ИЛИ» 2-й элемент сохраняет свои возможности по надежной реализации процесса в течение этого времени».

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

- для системы из двух последовательно соединенных элементов

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

- для системы из двух параллельно соединенных элементов

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

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

Рекурсивное применение соотношений (В.6), (В.7) снизу-вверх дает соответствующие вероятностные оценки для сколь угодно 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 формулам (В.6) или (В.7) проводится расчет вероятности нарушения надежности реализации процесса 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 формулам (В.6) или (В.7) 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.6) и (В.7). Полученный вид этой функции распределения, построенной по точкам (например, с использованием программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения надежности 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 сопровождения 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

$$T_{диаг}^{(2)} = T_{диаг}^{(1)} \cdot \left(1 - R^{(1)}\right) + R^{(1)} \cdot T_{восст}, \tag{В.8}$$

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, если время восстановления больше времени диагностики) или пессимистичным (если время восстановления заметно меньше времени диагностики при частых отказах);

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

$$T_{диаг}^{(r)} = T_{диаг}^{(r-1)} \cdot \left(1 - R^{(r-1)}\right) + R^{(r-1)} \cdot T_{восст}, \tag{В.9}$$

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.

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

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

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

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 сопровождения системы (в части, свойственной этому процессу).

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 логически 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 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 сопровождения 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 сопровождения системы;

β — среднее время развития угроз с момента возникновения источников угроз до нарушения нормальных условий (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 обеспечению 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:

$P_{возд}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$, $T_{зад}$) — вероятность отсутствия нарушения требований защите информации в моделируемой системе в течение периода $T_{зад}$.

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

Расчет показателей применительно к процессу сопровождения 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 сопровождения системы в течение задаваемого периода прогноза $R_{наруш}(T_{зад}) = R_{наруш}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$, $T_{зад}$) осуществляют как дополнение до единицы значения $P_{возд}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$, $T_{зад}$).

Примечание — При необходимости могут быть использованы 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

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

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

где $R_{надежн}(T_{зад})$ — вероятность нарушения надежности реализации процесса сопровождения системы в течение периода прогноза $T_{зад}$ без учета требований по защите информации, рассчитывается по моделям и рекомендациям В.2,

$R_{наруш}(T_{зад})$ — вероятность нарушения требований по защите информации для процесса сопровождения системы в течение периода прогноза $T_{зад}$, рассчитывается по моделям и рекомендациям В.3.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса сопровождения системы

Г.1 Общие положения

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

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

При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможными оценками ущербов.

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 моделируемой системе для прогнозирования рисков определению подлежат:

- состав выходных результатов и выполняемых действий процесса сопровождения системы и используемых при этом активов;
- перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для выходных результатов и выполняемых действий процесса сопровождения системы;
- иные объекты, используемые в прогнозировании рисков, при необходимости оценки их влияния на выполнение 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 и быстрая (по сравнению с частотой возникновения и 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 надежности реализации исследуемого процесса сопровождения системы без учета требований по защите информации и/или нарушения требований по защите информации и/или нарушения реализации рассматриваемого процесса сопровождения системы с учетом требований по защите информации за заданный период прогноза. Прогнозирование рисков осуществляется 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 по 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 В зависимости от целей прогнозирования рисков модели приложения В логически могут быть представлены в виде «черного ящика» или в виде сложной структуры. Для отдельных элементов сложной системы или при

ее огрубленном моделировании используют модель «черного ящика». 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» (см. В.2.4).

Г.3.3 Для каждого из элементов и для моделируемой системы в целом вводится пространство элементарных состояний (с учетом логических взаимосвязей элементов условиями «И», «ИЛИ»). Например, в приложении к прогнозированию интегрального риска нарушения реализации процесса с учетом требований по защите информации пространство элементарных состояний на временной оси может быть формально определено двумя основными состояниями:

- «Надежность реализации процесса сопровождения 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 сопровождения системы «И»/«ИЛИ» выполнение требований по защите информации в системе нарушено» — в противном случае.

В приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси может быть формально определено двумя другими основными состояниями:

- «Выполнение требований по защите информации в процессе сопровождения системы обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации, т. е. с точки зрения системной инженерии их невыполнение может привести к ущербу;
- «Выполнение требований по защите информации в процессе сопровождения системы нарушено» — в противном случае.

Г.3.4 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.3.2.

В Г.7 приведены примеры прогнозирования рисков.

Г.4 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе основными расчетными показателями являются (см. приложение В):

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

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

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

Применительно к моделируемой системе исходными являются данные, необходимые для проведения расчетов по моделям и рекомендациям В.2, В.3, В.4.

Г.5 Порядок прогнозирования рисков

Г.5.1 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 из В.2, В.3, В.4. Разрабатывают необходимые методики системного анализа, обеспечивающие более детальный учет особенностей процесса сопровождения системы (см. приложение Е). Осуществляют расчет выбранных показателей с использованием соотношений (В.1)—(В.11) и иных рекомендаций приложения В.

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.

Г.7 Примеры

Г.7.1 Приведенные примеры демонстрируют отдельные аналитические возможности методических указаний.

В период до 2035 года России предстоит многогранная работа по решению ряда приоритетных задач освоения Арктики [27], включая:

- задачи развития социально-экономической инфраструктуры, предусматривающие инфраструктурное обустройство минерально-сырьевых центров, создание эффективной системы предупреждения и ликвидации последствий аварийных разливов нефти и нефтепродуктов на всей протяженности Северного морского пути, развитие системы энергоснабжения, модернизации объектов локальной генерации;
- задачи развития транспортной инфраструктуры, предусматривающие формирование ледокольного, аварийно-спасательного и вспомогательного флотов, строительство и модернизацию морских портов, расширение сети аэропортов и посадочных площадок;
- задачи развития информационно-коммуникационной инфраструктуры, предусматривающие развитие систем и средств постоянного комплексного космического мониторинга Арктики, создание системы контроля за обеспечением безопасности судоходства.

При создании и последующей эксплуатации соответствующих инфраструктурных зданий и сооружений в Арктике неизбежно использование процесса их сопровождения с применением структурированной СМИС по ГОСТ Р 22.1.12. В свою очередь СМИС может стать неотъемлемой частью единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций.

В привязке к некоторым из функций СМИС, позволяющим достичь демонстрационные цели примеров настоящих методических указаний, проиллюстрирован прогноз:

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

Для определенности с точки зрения системной инженерии рассмотрен фрагмент варианта создания и функционирования СМИС в интересах решения задач развития социально-экономической, транспортной и информационно-коммуникационной инфраструктуры в Арктике. С учетом возможных ущербов цели прогнозирования рисков в примерах сформулированы следующим образом. В условиях существующей неопределенности предлагается осуществить:

- количественную оценку риска нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации;
- количественную оценку риска нарушения требований по защите информации;
- выявление критичных факторов, влияющих на риски;
- определение такого периода, при котором сохраняются гарантии удержания рисков в допустимых пределах;
- количественную оценку интегрального риска нарушения реализации процесса сопровождения системы с учетом требований по защите информации.

Вышеизложенное в Г.7.1 представляет собой выполнение шагов 1, 2 из Г.5.

Г.7.2 Пример 1 (см. Г.7.3) иллюстрирует прогноз рисков нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации с использованием модели СМИС, создаваемой и действующей с учетом рекомендаций ГОСТ Р 22.1.12 и 6.1.3. Пример 2 (см. Г.7.4) иллюстрирует прогноз риска нарушения требований по защите информации непосредственно в модели СМИС с ориентацией на ее функциональную структуру по ГОСТ Р 22.1.12, включающую ССП, СУКС и СМИК. Пример 3 (см. Г.7.5) дает представление об интегральном риске нарушения реализации процесса сопровождения системы с учетом требований по защите информации.

Полагая соизмеримость возможных ущербов, в примерах осуществлен системный анализ с использованием вероятностных показателей рисков.

Г.7.3 Пример 1. Моделируемая система примера 1, демонстрирующего прогнозирование риска нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации, представлена на рисунке Г.1. В качестве моделируемой системы выступает множество подсистем жизнеобеспечения и безопасности гипотетичного комплекса зданий и сооружений:

- систем вентиляции, кондиционирования, водоснабжения, канализации, электро- и газоснабжения (элемент 1);
- инженерно-технический комплекс пожарной безопасности объектов (элемент 2);
- лифтовое оборудование (элемент 3);
- система связи и оповещения (элемент 4);
- системы охранной сигнализации, видеонаблюдения, контроля и управления доступом, досмотровые средства (элемент 5);

- системы обнаружения повышенного уровня радиации, аварийных химически опасных веществ, биологически опасных веществ, значительной концентрации токсичных и взрывоопасных концентраций газовоздушных смесей (элемент 6).

Процесс сопровождения этой системы осуществляется с использованием модели СМИС. Все подсистемы ССП, СУКС и СМИК являются источниками данных для оценки жизнеобеспечения и безопасности рассматриваемого комплекса зданий и сооружений (системы), состояние которых отслеживается в рамках процесса сопровождения. Процесс сопровождения осуществляется с использованием аналитических возможностей СМИС, т. е. в рамках процесса сопровождения системы, состоящей из комплекса зданий и сооружений, используется процесс функционирования СМИС — см. 4.3 и ГОСТ Р 59355.

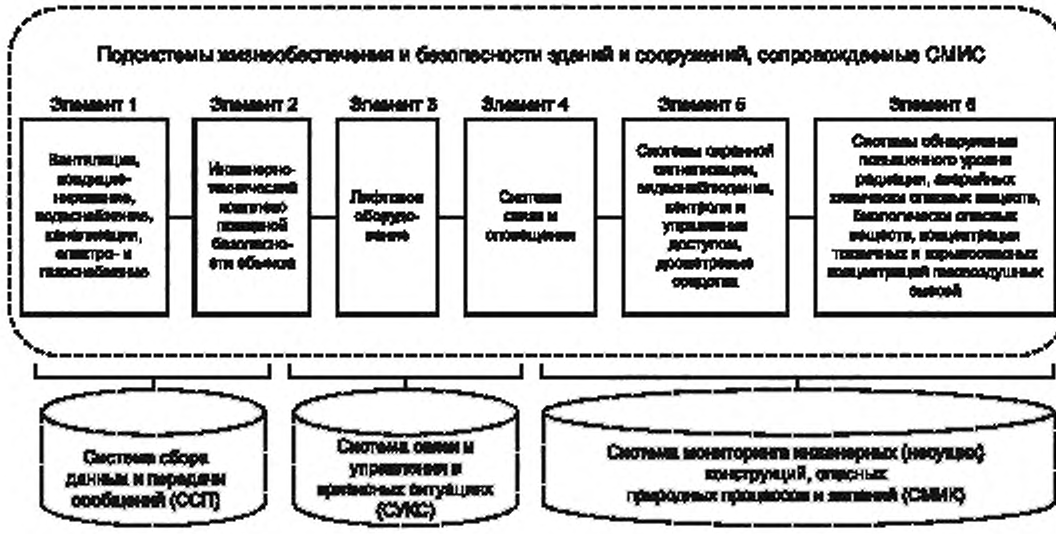

Рисунок Г.1 — Моделируемая система для примера 1

Применима следующая интерпретация: в течение задаваемого периода прогноза моделируемая система находится в элементарном состоянии «Целостность моделируемой системы сохранена» (это означает, что реализация процесса сопровождения системы обеспечивает надежное получение выходных результатов), если каждый из элементов 1—6 в течение всего периода находится в состоянии «Целостность элемента моделируемой системы сохранена». Тем самым для всех элементов обеспечена надежная реализация процесса сопровождения.

Прогнозирование риска нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации осуществлено с использованием рекомендаций подраздела В.2. Не вдаваясь в детали осуществляемых действий на уровне подсистем жизнеобеспечения и безопасности рассматриваемого комплекса зданий и сооружений, в таблице Г.1 отражены гипотетичные усредненные исходные данные с возможным обоснованием принятых значений для моделирования по моделям В.2. Для расчетов в качестве точечного периода прогноза выбран срок 2 года, который характерен для кратко- и среднесрочных планов реального создания и развития многих инфраструктурных проектов при освоении Арктики.

Таблица Г.1 — Исходные данные для прогнозирования риска нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации

Исходные данные	Элементы	Значения и комментарии
σ — частота возникновения источников угроз нарушения надежности реализации процесса для элемента	Элемент 1	4 раза в год, что соизмеримо с возникновением угроз, связанных с временными отклонениями от нормы значений параметров оборудования подсистем вентиляции, кондиционирования, водоснабжения, канализации, электро- или газоснабжения
	Элемент 2	1 раза в 5 лет, что соизмеримо со временем наработки на отказ оборудования комплекса пожарной безопасности объекта
	Элемент 3	1 раз в 10 лет, что соизмеримо со временем наработки на отказ лифтового оборудования

Окончание таблицы Г.1

Исходные данные	Элементы	Значения и комментарии
	Элемент 4	1 раз в 2 года, что соизмеримо со временем наработки на отказ системы связи и оповещения
	Элемент 5	1 раз в 5 лет, что соизмеримо со временем наработки на отказ охранной сигнализации, видеонаблюдения, контроля и управления доступом, досмотровые средства
	Элемент 6	1 раз в год, что соизмеримо с возникновением угроз повышения уровня радиации, аварийных химически опасных веществ, биологически опасных веществ, значительной концентрации токсичных и взрывоопасных концентраций газовоздушных смесей
β — среднее время развития угроз для элемента с момента возникновения источников угроз до нарушения с возможным ущербом	По всем элементам 1 — 6	1 нед — это время до возможного недопустимого ущерба после возникновения первых признаков угроз
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей элемента	Элемент 1	2 мин — определяется скважностью сбора данных о состоянии оборудования зданий и сооружений в системах дистанционного контроля
	Элемент 2	1 мин — определяется чувствительностью датчиков комплекса пожарной безопасности объекта
	Элемент 3	8 ч — определяется регламентом сменной работы при обслуживании лифтового оборудования
	Элемент 4	10 мин — определяется частотой обращения пользователей к средствам системы связи и оповещения
	Элемент 5	1 ч — определяется спецификой работы с оборудованием охранной сигнализации, видеонаблюдения, контроля и управления доступом, досмотровыми средствами
	Элемент 6	1 ч — определяется периодичностью ручного (или не полностью автоматического) сбора данных, связанных с измерениями уровня радиации, аварийных химически опасных веществ, биологически опасных веществ, концентрации токсичных и взрывоопасных концентраций газовоздушных смесей
$T_{диаг}$ — среднее время диагностики состояния элемента	По всем элементам 1—6	1 мин, что соизмеримо с реакцией диспетчера на критичные отклонения значений мониторируемых параметров
$T_{восст}$ — среднее время приемлемого восстановления элемента после выявления нарушений	По всем элементам 1—6	1 сут (для легкоустранимых нарушений, в т. ч. с использованием технологий автоматического и автоматизированного управления)
$T_{зад}$ — задаваемая длительность периода прогноза	По всем элементам 1—6	От 1 года до 4-х лет работы по освоению Арктики (для определения периода, при котором сохраняются гарантии удержания в допустимых пределах риска нарушения требований по защите информации)

Анализ результатов моделирования показал, что в вероятностном выражении расчетный риск нарушения надежности реализации процесса сопровождения системы в течение двух лет составит 0,135 (за все элементы), в т. ч. по элементам с 1-го по 5-й — не выше 0,005, а по 6-му элементу 0,128 (см. рисунок Г.2). Это свидетельствует о том, что сбор данных явно представляет собой «узкое место» в системах обнаружения повышенного уровня радиации, аварийных химически опасных веществ, биологически опасных веществ, концентрации токсичных и взрывоопасных концентраций газовоздушных смесей (элемент 6 моделируемой системы). В свою очередь для

прогноза на 4 года вероятность нарушения требований по защите информации за все действия СМИС (т. е. по всем элементам 1—6) составит около 0,25, а для прогноза на 1 год вероятность нарушения требований по защите информации составит 0,07 (см. рисунок Г.3).

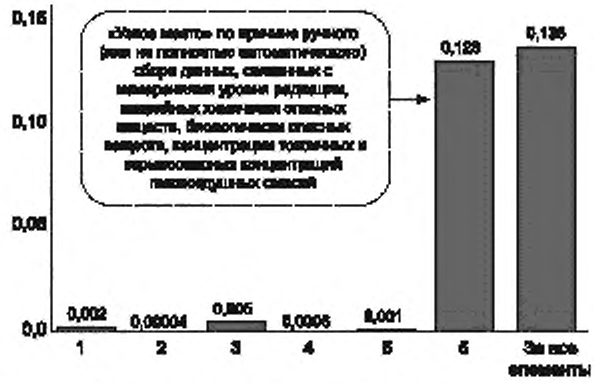

Рисунок Г.2 — Риски нарушения надежности реализации процесса сопровождения системы в течение 2 лет (при частоте сбора данных по 6-му элементу 1 раз в час)

Рисунок Г.3 — Зависимость риска нарушения надежности реализации процесса сопровождения системы от длительности периода прогноза (от 1 до 4 лет)

Одним из критичных факторов для систем обнаружения повышенного уровня радиации, аварийных химически опасных веществ, биологически опасных веществ, концентрации токсичных и взрывоопасных концентраций газовоздушных смесей является ручной (или не полностью автоматический) сбор данных измерений, что приводит к обновлению данных 1 раз в час (см. параметр $T_{исх}$ в таблице Г.1). За счет осуществления полной автоматизации процедуры сбора этих данных для элемента 6 возможно сокращение среднего времени между окончанием предыдущей и началом очередной диагностики состояния соответствующих параметров до уровня 2-х мин аналогично скважности сбора данных о состоянии оборудования зданий и сооружений в системах дистанционного контроля для элемента 1 из таблицы Г.1. За счет этого при прочих неизменных условиях функционирования СМИС возможно снижение риска нарушения надежности реализации процесса сопровождения системы (за все элементы) в 15 раз: с уровня 0,135 до уровня 0,009. Достаточно сравнить риски на рисунках Г.2 и Г.4. Возможность достижения такого существенного эффекта выявлена на основе прогнозирования рисков с применением моделей и рекомендаций В.2.

Для прогноза на 1 год вероятность нарушения требований по защите информации составит 0,004 (см. рисунок Г.5). В свою очередь в результате анализа расчетной зависимости риска от длительности периода прогноза (от 1 до 4 лет) дополнительно установлено, что в условиях примера при сборе данных измерений по 6-му элементу 1 раз в каждые 2 мин уровень риска 0,10 не будет превышен в течение 2,4 лет. Это означает, что, ориентируясь на задаваемый допустимый риск нарушения надежности реализации процесса сопровождения системы без учета требований по защите информации на уровне 0,010, в условиях примера в течение 2,4 лет будут сохранены гарантии удержания риска в допустимых пределах. Это в 1,71 раза дольше по сравнению с аналогичным гарантийным сроком, рассчитанным для гораздо более высокого допустимого риска 0,10 в условиях ручного (или не полностью автоматического) сбора данных измерений — см. рисунок Г.3.

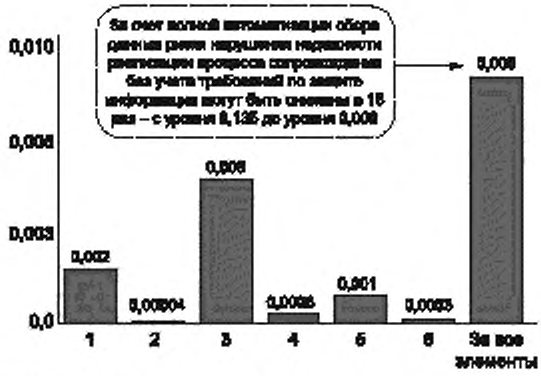

Рисунок Г.4 — Риски нарушения надежности реализации процесса сопровождения системы в течение 2 лет (при частоте сбора данных по 6-му элементу 1 раз каждые 2 мин)

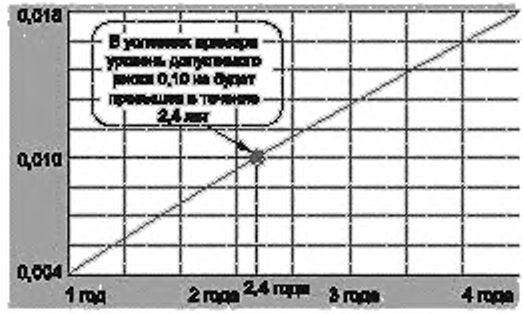

Рисунок Г.5 — Зависимость риска нарушения надежности реализации процесса сопровождения системы от длительности периода прогноза (от 1 до 4 лет)

Г.7.4 Пример 2. Моделируемая система примера 2, демонстрирующего прогнозирование риска нарушения требований по защите информации в процессе сопровождения системы, т. е. в самой СМИС, представлена на рисунке Г.6. Моделируемая система уже иная, она представляет собой комплекс действий, осуществляемых взаимодействующими системами СМИС: ССП, СУКС и СМИК. Все три элемента объединены логическим условием «И». Применима следующая интерпретация: в течение задаваемого периода прогноза моделируемая система находится в элементарном состоянии «Выполнение требований по защите информации в системе обеспечено», если в течение всего периода ССП «И» СУКС «И» СМИК находятся в состоянии «Выполнение требований по защите информации для элемента обеспечено».

Прогнозирование риска нарушения требований по защите информации осуществлено с использованием рекомендаций В.3. Не вдаваясь в детали осуществляемых действий на уровне систем ССП, СУКС и СМИК, в таблице Г.2 отражены гипотетичные усредненные исходные данные с возможным обоснованием принятых значений для моделирования по моделям В.3. Для сохранения преемственности с примером 1 в качестве точечного периода прогноза по-прежнему выбран срок 2 года, характерный для среднесрочных планов реального создания и развития многих инфраструктурных проектов по освоению Арктики.

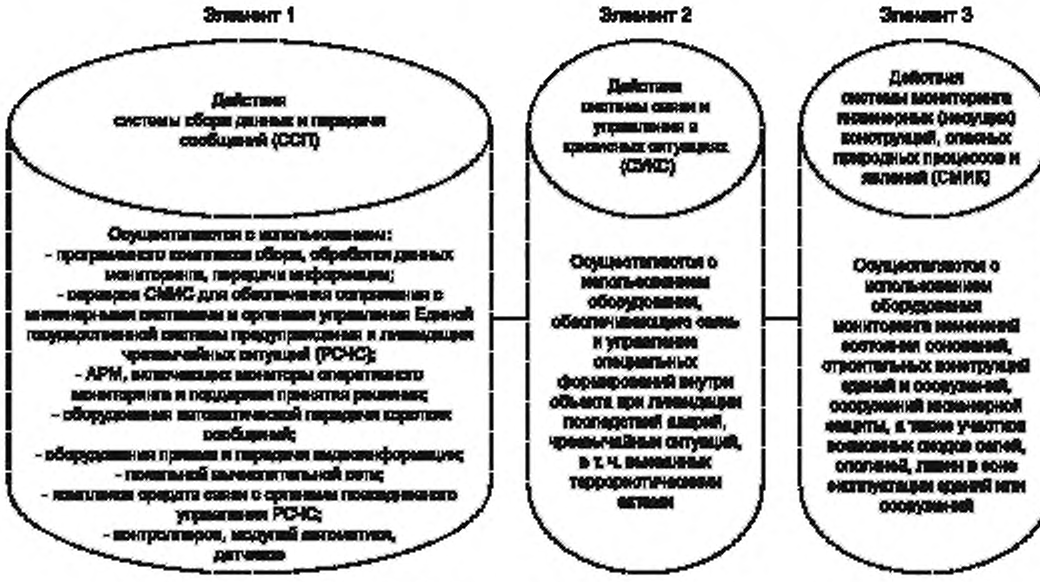

Рисунок Г.6 — Моделируемая система для примера 2

Таблица Г.2 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе сопровождения комплекса зданий и сооружений

Исходные данные	Элементы	Значения и комментарии
α — частота возникновения источников угроз нарушения требований по защите информации	Элемент 1 ССП	2 раза в год, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения сбора данных и передачи сообщений
	Элемент 2 СУКС	4 раза в год, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения для системы связи и управления
	Элемент 3 СМИП	12 раз в год, что соизмеримо с возникновением угроз от использования импортного технического и программного обеспечения (не сертифицированного по требованиям безопасности) при обеспечении мониторинга инженерных конструкций, опасных природных процессов и явлений
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	По всем элементам 1—3	1 мес (на некоторых примерах вредоносного программного обеспечения предполагается, что источники угроз активизируются не сразу, а с некоторой задержкой не менее месяца) — это время до возможного ущерба после возникновения первых признаков угроз
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	Элемент 1 ССП	8 ч — определяется регламентом контроля целостности активов ССП
	Элемент 2 СУКС	8 ч — определяется регламентом контроля целостности программного обеспечения и активов СУКС
	Элемент 3 СМИП	1 ч — определяется регламентом контроля целостности программного обеспечения и активов СМИП
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы	По всем элементам 1—3	1 мин, что соизмеримо с длительностью автоматического контроля целостности программного обеспечения и активов ССП, СУКС, СМИП

Окончание таблицы Г.2

Исходные данные	Элементы	Значения и комментарии
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	По всем элементам 1—3	30 мин, включая перезагрузку программного обеспечения и восстановление данных ССП, СУКС, СМИП
$T_{зад}$ — задаваемая длительность периода прогноза	По всем элементам 1—3	От 1 года до 4 лет работы по освоению Арктики (для определения периода, при котором сохраняются гарантии удержания в допустимых пределах риска нарушения требований по защите информации)

Анализ результатов моделирования показал, что в вероятностном выражении риск нарушения требований по защите информации в течение двух лет составит для СМИС 0,079 (т. е. за все элементы — ССП, СУКС, СМИП), не превышая по каждому из элементов уровня 0,05 (см. рисунок Г.7). В свою очередь для прогноза на 4 года вероятность нарушения требований по защите информации за все действия СМИС составит около 0,15, а для прогноза на 1 год эта вероятность составит около 0,04 (см. рисунок Г.8). При проведении системного анализа выявлен важный результат: риск нарушения требований по защите информации для СМИП существенно ниже, нежели для ССП «И» СУКС. Это несмотря на то, что частота возникновения источников угроз для СМИП 12 раз в год вдвое превышает суммарную частоту возникновения угроз для ССП (2 раза в год) и СУКС (4 раза в год). Такой эффект достигается благодаря более частой диагностике возможностей системы по выполнению требований по защите информации (см. значения $T_{меж}$ в таблице Г.2).

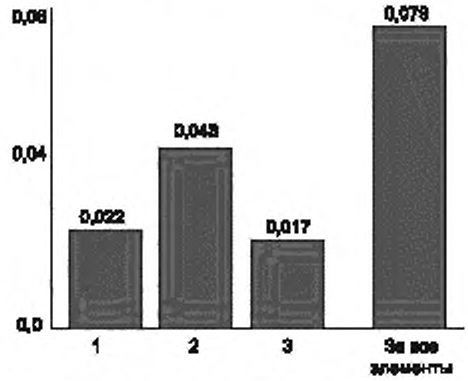

Рисунок Г.7 — Риски нарушения требований по защите информации по элементам 1—3 и за все элементы в течение 2 лет

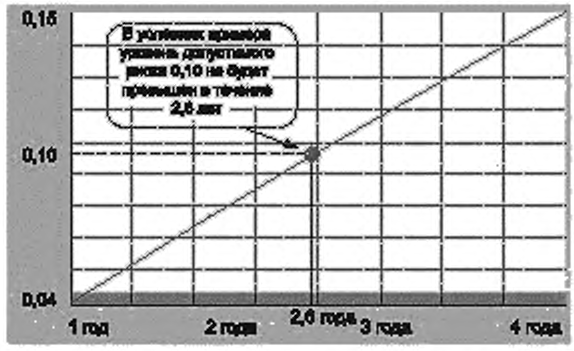

Рисунок Г.8 — Зависимость риска нарушения требований по защите информации по всем элементам СМИС от длительности периода прогноза (от 1 до 4 лет)

В результате анализа расчетной зависимости риска от длительности периода прогноза (от 1 до 4-х лет) дополнительно установлено, что в условиях примера допустимый уровень риска 0,10 не будет превышен в течение 2,6 лет. Это означает, что, ориентируясь для процесса сопровождения системы при освоении Арктики на задаваемый допустимый риск нарушения требований по защите информации на уровне 0,010, в условиях примера в течение 2,6 лет будут сохранены гарантии удержания риска в этих допустимых пределах.

Г.7.5 Пример 3. В продолжение примеров 1, 2 интегральный риск $R_{интегр}(T_{зад})$ нарушения реализации процесса сопровождения системы с учетом требований по защите информации рассчитан с использованием рекомендаций раздела В.4 для периода прогноза $T_{зад} = 1$ год.

По результатам примера 1 $R_{надежн}(T_{зад}) = 0{,}004$ (см. рисунок Г.5), а по результатам примера 2 $R_{наруш}(T_{зад}) = 0{,}04$ (см. рисунок Г.8). Тогда по формуле (В.10)

$$R_{интегр}(T_{зад}) = 1 - (1 - 0{,}004) \cdot (1 - 0{,}04) \approx 0{,}044.$$

В итоге интегральный риск нарушения реализации процесса сопровождения системы в течение года с учетом требований по защите информации не превысит 0,05. В общем случае такой уровень риска может быть признан приемлемым по прецедентному принципу. Вместе с тем по результатам системного анализа установлено: в условиях примеров существуют дополнительные реальные возможности снижения рисков, например, путем применения организационно-технических мер по повышению частоты диагностики возможностей системы по выполнению требований по защите информации.

Принятие решений по способам снижения рисков должно быть количественно обосновано с использованием моделей, методов и методик, рекомендуемых в приложениях В, Г, Д, Е или иными приемлемыми методами.

Примечание — Другие 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.

Г.8 Материально-техническое обеспечение

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

- конструкторская и эксплуатационная документация для сопровождаемой системы (используют при формировании необходимых исходных данных для моделирования);
- модель угроз безопасности информации (используют при формировании необходимых исходных данных для моделирования 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 при формировании необходимых исходных данных для моделирования);
- планы ликвидации нарушений, инцидентов и аварий, связанных с нарушением требований по защите информации, и восстановления целостности системы (используют при формировании необходимых исходных данных для моделирования и обоснования усовершенствований в результате решения задач системного анализа);
- обязанности должностных лиц и инструкции по защите информации при выполнении процесса (используют при формировании необходимых исходных данных для моделирования 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.9 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 сопровождения 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 сопровождения 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.

Требования системной инженерии при принимаемых рисках, свойственных системе-эталону, являются наиболее жесткими, они не учитывают специфики рассматриваемой системы, а ориентируются лишь на мировые технические и технологические достижения для удовлетворения требований заинтересованных сторон и рационального решения задач системного анализа. Полной проверке на соответствие этим требованиям подлежит система в целом, составляющие ее подсистемы и реализуемые процессы жизненного цикла. Выполнение этих требований является гарантией обеспечения высокого качества и безопасности 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 по другим соображениям) или невозможной ориентация на допустимые риски, свойственные системе-эталону. Вследствие этого минимальной гарантией обеспечения качества и безопасности выполнения процесса сопровождения системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Типовые допустимые значения количественных показателей рисков для процесса сопровождения 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 выполнения процесса сопровождения системы 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 сопровождения системы	Не выше 0,05	Не выше 0,01
Интегральный риск нарушения реализации процесса сопровождения 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 сопровождения системы

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

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

Е.4 Методики выявления явных и скрытых недостатков процесса сопровождения системы с использованием прогнозируемых рисков.

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

Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса сопровождения системы.

Примечания

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

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 года № 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)

[27] «Основы государственной политики Российской Федерации в Арктике на период до 2035 года». (Утверждены Указом Президента РФ от 5 марта 2020 г. № 164)

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

Ключевые слова: актив, безопасность, защита информации, модель, риск, системная инженерия, процесс сопровождения системы, управление

Технический редактор *И.Е. Черепкова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 19.05.2021. Подписано в печать 31.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 5.12. Уч.-изд. л. 4,60.

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