ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59354— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ АТТЕСТАЦИИ 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 30 апреля 2021 г. № 335-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, функционирования, сопровождения, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357. Для процесса аттестации системы — по настоящему стандарту.

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ АТТЕСТАЦИИ СИСТЕМЫ

System engineering. Protection of information in system validation process

Дата введения — 2021—11—30

1 Область применения

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

Для практического применения в приложениях А—Д приведены примеры перечней активов, подлежащих защите, и угроз, типовые модели и методы прогнозирования рисков, типовые допустимые значения для показателей рисков, примерный перечень методик системного анализа.

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

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

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.051 Единая система конструкторской документации. Электронные документы. Общие положения

ГОСТ 2.102 Единая система конструкторской документации. Виды и комплектность конструкторских документов

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

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

Издание официальное

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

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

ГОСТ Р ИСО 3534-1 Статистические методы. Словарь и условные обозначения. Часть 1. Общие статистические термины и термины, используемые в теории вероятностей

ГОСТ Р ИСО 3534-2 Статистические методы. Словарь и условные обозначения. Часть 2. Прикладная статистика

ГОСТ Р ИСО 7870-1 Статистические методы. Контрольные карты. Общие принципы

ГОСТ Р ИСО 7870-2 Статистические методы. Контрольные карты. Часть 2. Контрольные карты Шухарта

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО/МЭК 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 27003 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 50779.41 (ИСО 7873—93) Статистические методы. Контрольные карты для арифметического среднего с предупреждающими границами

ГОСТ Р 50779.70 (ИСО 28590:2017) Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Введение в стандарты серии ГОСТ Р ИСО 2859

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

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

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

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

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

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

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

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

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 59329 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 59355 Системная инженерия. Защита информации в процессе функционирования системы

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 указа-

телю «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 ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р 51897, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

аттестация (валидация): Подтверждение (на основе представления объективных подтверждений) того, что требования, предназначенные для конкретного использования или применения, выполнены.

Примечание — Валидация в контексте жизненного цикла представляет собой совокупность действий, гарантирующих и обеспечивающих уверенность в том, что система способна реализовать свое предназначение, текущие и перспективные цели.

[ГОСТ Р 57193—2016, пункт 4.1.51]

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.3

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

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

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

[ГОСТ Р 57193—2016, пункт 4.1.42]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.5

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.6

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.7

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

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

3.1.10

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.11

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.12

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.13 **система-эталон:** Реальная или гипотетичная система, которая по своим показателям интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации принимается в качестве эталона для полного удовлетворения требований заинтересован-

ных сторон системы и рационального решения задач системного анализа, связанных с обоснованием допустимых рисков, обеспечением нормы эффективности защиты информации, обоснованием мер, направленных на достижение целей процесса, противодействие угрозам и определение сбалансированных решений при средне- и долгосрочном планировании, а также с обоснованием предложений по совершенствованию и развитию системы защиты информации.

3.1.14

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.1.15

требование по защите информации: Установленное правило или норма, которые должны быть выполнены при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

[ГОСТ Р 50922—2006, статья 2.9.2]

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

3.1.17

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использовано сокращение:

ТЗ — техническое задание.

Основные положения системной инженерии по защите информации в процессе аттестации системы

4.1 Общие положения

Организации используют процесс аттестации (валидации) системы в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения уверенности в том, что система отвечает требованиям по своему назначению и обладает возможностями достижения текущих и перспективных целей.

При реализации процесса аттестации системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должно быть обеспечено надежное выполнение процесса.

Для прогнозирования интегрального риска нарушения реализации процесса и обоснования эффективных предупреждающих мер по снижению этого риска или удержанию его в допустимых пределах используют системный анализ процесса с учетом требований по защите информации.

Определение выходных результатов процесса аттестации системы и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р 51904, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Оценку интегрального риска нарушения реализации процесса с учетом требований по защите информации осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59355. При этом учитывают специфику аттестуемой системы (см., например, [20]—[26]).

4.2 Стадии и этапы жизненного цикла систем

В общем случае процесс аттестации системы используют на стадиях разработки (модернизации, развития), эксплуатации и сопровождения системы после того, как система будет спроектирована, реализована или верифицирована. Процесс аттестации системы направлен на обеспечение объективных доказательств того, что система при своем применении будет выполнять (при ее разработке, модернизации, развитии, сопровождении) или выполняет (при эксплуатации) требования заинтересованных сторон, достигая намеченного использования в заданной эксплуатационной среде.

Стадии и этапы работ устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле систем формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839. Процесс аттестации системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости включать в себя другие процессы.

4.3 Цели процесса и назначение мер защиты информации

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

В общем случае главной целью процесса аттестации системы является предоставление объективных доказательств того, что при применении в заданной эксплуатационной среде система обеспечит выполнение заданных требований заинтересованных сторон. Основная задача аттестации состоит в приобретении уверенности заинтересованных сторон в возможностях системы согласно ее функциональному назначению.

4.3.2 Меры защиты информации в процессе аттестации системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, 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 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59346, ГОСТ Р МЭК 61508-7, [20]—[24] с учетом специфики аттестуемой системы и реализуемой стадии жизненного цикла.

4.4 Основные принципы

При проведении системного анализа процесса аттестации системы руководствуются основными принципами, определенными в ГОСТ Р 59349 с учетом дифференциации требований по защите информации в зависимости от категории значимости системы и важности обрабатываемой в ней информации (см. ГОСТ Р 59346, [19]—[24]). Все применяемые принципы подчинены принципу целенаправленности осуществляемых действий в планируемых и реализуемых процессах на протяжении всего жизненного цикла системы.

4.5 Основные усилия для обеспечения защиты информации

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

- на обеспечении готовности системы к выполнению требований заинтересованных сторон;
- 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 аттестации системы

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы (в качестве которой может выступать система защиты информации), в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований по защите информации формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например, [20]—[24]), 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 аттестации системы и поддержке при этом эффективности защиты информации.

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

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

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

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

- гарантированное подтверждение достаточности автоматизированной деклассификации конфиденциальной информации (в частности, анонимизации и 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);
- 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 и действия по защите информации должны охватывать активы, информация которых или о которых необходима для получения выходных результатов и выполнения действий процесса аттестации системы.

Примечание — В состав защищаемых активов могут быть включены активы иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика — например, привлекаемые средства измерений.

5.5 Определение активов, информация которых или о которых подлежит защите, определение перечня потенциальных угроз и формирование возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 59346, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, [20]—[24].

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

5.6 Эффективность защиты информации при выполнении процесса аттестации 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 осуществляют с использованием методов, моделей и методик (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, [20] — [24].

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 аттестации системы определен в 6.3.

Типовые модели и методы прогнозирования рисков в процессе аттестации системы, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д. Характеристики мер защиты информации и действий по защите информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам 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 аттестации системы, к которым предъявлены определенные требования по защите информации, выполняют оценку эффективности защиты информации на основе прогнозирования рисков в условиях возможных угроз.

6.1.2 В общем случае основными выходными результатами процесса аттестации системы являются:

- критерии аттестации системы относительно выполнения требований заинтересованных сторон;
- ограничения и допущения при аттестации системы, которые влияют на системные требования, архитектуру или проект системы;
- непосредственно отчетные материалы по аттестации системы и/или системных элементов;
- обеспечивающие системы или услуги, необходимые для аттестации;
- задокументированные результаты аттестации системы и выявленные отклонения;
- объективные доказательства того, что при применении в заданной эксплуатационной среде система обеспечит выполнение требований заинтересованных сторон с достижением поставленных целей;
- карта прослеживаемости системных элементов к требованиям заинтересованных сторон и системным требованиям при проведении аттестации системы.

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

- подготовительные действия:
  - определение области аттестации и соответствующих действий процесса аттестации системы, включая требования заинтересованных сторон, подлежащие количественной оценке, определение системы и/или системного элемента, подлежащего аттестации, ожидаемые результаты использования системы и/или системного элемента (например, аттестации могут подлежать описание замысла или документ, сценарий эксплуатации, модель, макет или прототип системы),
  - определение ограничений по выполнению действий процесса аттестации системы, включая ограничения по технической выполнимости, стоимости, времени, пригодности к аттестации видов обе-

спечения или квалифицированного персонала, договорные ограничения, учитывающие в том числе специфику системы,

- выбор или разработку соответствующих методов и методик, определение условий и критериев для каждого действия процесса аттестации с учетом специфики системы, целей проекта и допустимых рисков,

- определение стратегии аттестации системы, включая определение соотношения между областью аттестации, ограничениями и методами выполнения действий процесса аттестации с привлечением обеспечивающих систем (моделей, испытательных стендов, тренажеров, компетентного персонала, вспомогательных услуг),

- определение ограничений системы, вытекающих из стратегии аттестации системы, для их включения в требования заинтересованных сторон, в том числе ограничения, связанные с точностью, неопределенностью, воспроизводимостью, методами измерений, пригодностью, доступностью и взаимодействиями,

- определение и планирование действий относительно обеспечивающих систем или вспомогательных услуг, которые необходимы для поддержки аттестации системы,

- получение или приобретение доступа к обеспечивающим системам или вспомогательным услугам для поддержки аттестации системы, включая при необходимости заключение договоров субподряда, закупку, разработку, повторное использование;

- проведение непосредственно аттестации системы, включая:

- выполнение процедуры аттестации системы согласно принятой стратегии в среде, близкой к эксплуатационной среде или ее виртуальному представлению с определенными обеспечивающими системами и ресурсами,

- рассмотрение результатов аттестации системы с целью подтверждения функциональной готовности системы относительно выполнения требований заинтересованных сторон,

- документирование результатов аттестации системы и выявленных отклонений, включая отклонения из-за некорректностей в принятой стратегии аттестации, обеспечивающих системах, процедурах аттестации,

- регистрацию эксплуатационных инцидентов, выявленных проблем и гарантий того, что они практически разрешаемы,

- обеспечение прослеживаемости системных элементов, прошедших аттестацию, и стратегии аттестации, архитектуры системы, проекта и системных требований.

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

6.2 Требования к составу показателей

Выбираемые показатели должны обеспечивать проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения реализации процесса аттестации системы с учетом требований по защите информации.

Эффективность защиты информации оценивают с помощью количественных показателей, которые позволяют сформировать представление о текущих и потенциальных проблемах или о возможных причинах недопустимого снижения эффективности на ранних этапах проявления явных и скрытых угроз безопасности информации, когда можно принять предупреждающие корректирующие 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 аттестации системы используют следующие количественные показатели:

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

6.3.2 Риск нарушения надежности реализации процесса аттестации системы без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации этого процесса без учета требований по защите информации (в зависимости от вероятности невыполнения необходимых действий процесса и вероятности нарушения необходимой готовности системы к выполнению требований заинтересованных сторон) в сопоставлении с возможным ущербом.

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

6.3.4 Интегральный риск нарушения реализации процесса аттестации системы с учетом требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса без учета защиты информации и вероятностью нарушения требований по защите информации (см. В.2, В.3, В.4 приложения В) в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

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

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к системному анализу

Требования к системному анализу процесса аттестации системы включают:

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

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

При обосновании и формулировании конкретных требований к системному анализу дополнительно руководствуются положениями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, 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/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики аттестуемой системы (см., например, [21]—[24]).

Примечание — Примеры решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

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

- выходные результаты процесса (см. 6.1.2);
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации (см. [21]—[24]);
- договоры и соглашения на проведение работ по созданию (модернизации, развитию) и аттестации системы;
- лицензии, подтверждающие право поставщика (производителя) на проведение работ по созданию (модернизации, развитию) и аттестации системы;
- финансовые и плановые документы, связанные с проведением работ по созданию (модернизации, развитию) и аттестации системы;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем — см. ГОСТ 34.601);
- документацию при выполнении научно-исследовательских работ (см. ГОСТ 7.32, ГОСТ 15.101) с учетом специфики аттестуемой системы;
- конструкторскую и технологическую документацию (для создаваемой, модернизируемой или применяемой системы — см. ГОСТ 2.051, ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201);
- эксплуатационную и ремонтную документацию (см. ГОСТ 2.602, ГОСТ 34.201, ГОСТ Р 2.601) с учетом специфики аттестуемой системы;
- технические задания (см. 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 ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

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

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию (см. 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 (см. [21]—[24]);
- угрозы безопасности функционирования программного обеспечения, оборудования и коммуникаций, используемых в процессе работы (см. ГОСТ Р ИСО/МЭК 27002 и ГОСТ Р 54124);
- угрозы безопасности информации при подготовке и обработке документов (см. ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412);
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика — см. ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С);
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному заказчику, информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги (см. ГОСТ Р ИСО/МЭК 27036-4);
- прочие соответствующие угрозы безопасности информации и уязвимости для информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов из Банка данных угроз, сопровождаемого государственным регулятором.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе аттестации системы могут применяться любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Применение типовых методов и моделей настоящего стандарта обеспечивает оценку следующих показателей:

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

В.1.2 Риск нарушения надежности реализации процесса аттестации системы без учета требований по защите информации характеризуют:

- риском невыполнения необходимых действий процесса, определяемым вероятностью невыполнения необходимых действий процесса;
- риском нарушения готовности системы к выполнению требований заинтересованных сторон, определяемым вероятностью нарушения готовности системы к выполнению требований заинтересованных сторон системы.

Риск нарушения требований по защите информации в процессе аттестации системы определяют соответствующей вероятностью нарушения требований по защите информации.

Вероятностные оценки обеспечивают уровень адекватности, достаточный для решения задач системного анализа, при условии многократной повторяемости анализируемых событий или в предположении такой повторяемости.

В.1.3 Интегральный риск нарушения реализации процесса аттестации системы с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса аттестации системы без учета требований по защите информации и риска нарушения требований по защите информации в этом процессе.

В.1.4 При оценке рисков расчетным вероятностным показателям сопоставляют возможный ущерб, оцениваемый тяжестью последствий для системы и заинтересованных сторон в случае реализации угроз.

В.1.5 Для моделируемой системы нарушение реализации процесса аттестации системы с учетом требований по защите информации характеризуется переходом системы в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: либо из-за невыполнения необходимых действий процесса, либо из-за нарушения готовности системы к выполнению требований заинтересованных сторон, либо из-за нарушения требований по защите информации, либо из-за комбинации перечисленных причин.

В.1.6 В общем случае, исходя из целей системного анализа, риски оценивают на разных исходных данных. При использовании одних и тех же моделей для расчетов это может приводить к различным оценкам и интерпретациям рисков. Различия связаны с неодинаковой тяжестью возможного ущерба для заинтересованных сторон (из-за невыполнения необходимых действий процесса, нарушения готовности системы к выполнению требований заинтересованных сторон, нарушений требований по защите информации), недоступностью или неполнотой статистических данных, используемых каждой из этих сторон в качестве исходных данных при системном анализе.

В.1.7 Выполнение или невыполнение действий и требований при моделировании отслеживается с использованием индикаторной функции *Ind* (α), которая позволяет учесть критичность последствий, связанных с невыполнением заданных условий согласно собираемой статистике:

$$Ind(\alpha) = \begin{cases} 1, & \text{если условие } \alpha \text{ выполнено,} \\ 0, & \text{если условие } \alpha \text{ не выполнено.} \end{cases} \quad (В.1)$$

Условие α, используемое в индикаторной функции, формируют путем анализа выполнения конкретных условий, существенных для процесса аттестации системы.

В.1.8 При формировании исходных данных для моделирования и проведении разностороннего системного анализа используют статистические методы контроля по ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р 50779.41, ГОСТ Р 50779.70, методы оценки рисков из настоящего приложения и/или по 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 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, ГОСТ Р МЭК 62264-1.

В.2 Методы оценки рисков нарушения надежности реализации процесса аттестации системы без учета требований по защите информации

В.2.1 Общие положения

В настоящем подразделе приведены методы оценки частных и обобщенного рисков нарушения надежности реализации процесса аттестации системы без учета требований по защите информации.

Частные риски характеризуются сопоставляемыми возможными затратами, ущербами и вероятностями соответствующих событий:

- невыполнения необходимых действий процесса аттестации системы;
- нарушения готовности системы к выполнению требований заинтересованных сторон.

В.2.2 Оценка риска невыполнения необходимых действий процесса аттестации

В.2.2.1 В процессе аттестации системы должны быть выполнены необходимые действия. Невыполнение (в том числе незавершение выполнения) необходимых действий процесса — это угроза возможного ущерба. В общем случае требования к завершенности необходимых действий процесса формулируют на уровне стратегии, процедур и методик аттестации системы, принятых условий и ограничений.

В.2.2.2 При оценке риска вычисляют вероятность невыполнения необходимых действий процесса аттестации системы. На основе применения статистических данных вероятность $R_{\text{действий}}(T_{\text{зад}})$ невыполнения необходимых действий процесса за задаваемое время $T_{\text{зад}}$ вычисляют по формуле

$$R_{\text{действий}}(T_{\text{зад}}) = G_{\text{невыполн}}(T_{\text{зад}}) / G(T_{\text{зад}}), \quad \text{(В.2)}$$

где $G_{\text{невыполн}}(T_{\text{зад}})$ и $G(T_{\text{зад}})$ — соответственно количество случаев невыполнения необходимых действий процесса и общее количество необходимых действий, подлежащих выполнению в процессе аттестации системы за заданное время $T_{\text{зад}}$ согласно статистическим данным.

Условие выполнения (включая завершение выполнения) необходимых действий определено как условие непревышения максимально допустимого уровня, задаваемого для вероятности невыполнения необходимых действий процесса аттестации системы $R_{\text{доп. действий}}(T_{\text{зад}})$.

Это условие выражается в форме: $R_{\text{действий}}(T_{\text{зад}}) \le R_{\text{доп. действий}}(T_{\text{зад}})$. В выражении для обобщенного риска показатель завершенности выполнения необходимых действий для процесса аттестации системы $Z_{\text{действий}}(T_{\text{зад}})$ определен следующим образом:

$$Z_{\text{действия}}(T_{\text{зад}}) = \begin{cases} 0, & \text{если условие завершения необходимых действий выполнено;} \\ R_{\text{действий}}(T_{\text{зад}}) \text{ по (В.2)}, & \text{если условие не выполнено или не задано.} \end{cases} \quad \text{(В.3)}$$

В.2.3 Оценка риска нарушения готовности системы к выполнению требований заинтересованных сторон

В.2.3.1 В условиях существующих неопределенностей оценивают вероятностные показатели нарушения готовности системы к выполнению меняющихся со временем требований заинтересованных сторон по качеству, срокам и затратам. Это позволяет определить показатели удовлетворенности заинтересованных сторон для последующей оценки обобщенного риска нарушения надежности реализации процесса аттестации системы без учета требований по защите информации.

В.2.3.2 Для оценки вероятности нарушения готовности системы к выполнению требований заинтересованных сторон по качеству и срокам используют модель, учитывающую изменение во времени потребностей и требований заинтересованных сторон. При аттестации проверяется готовность системы к выполнению формальных требований, на реализацию которых были затрачены время и ресурсы, но которые естественным образом устаревают с течением времени и изменяются. В итоге функциональные возможности аттестуемой системы могут оказаться реально невостребованными из-за рассогласования изменившихся требований заинтересованных сторон и реализованных функциональных возможностей системы. Востребованными на момент аттестации признают такие функциональные возможности системы, использование которых способно в заданных условиях обеспечить удовлетворенность заинтересованных сторон. Более актуальные потребности и требования заинтересованных сторон призваны заменить устаревшие требования к системе, но на их реализацию требуются время и дополнительные ресурсы. В свою очередь согласованные измененные потребности и требования заинтересованных сторон сами также могут меняться со временем. Таким образом на временной оси на момент аттестации возникают ситуации готовности системы к выполнению требований заинтересованных сторон по качеству и срокам и нарушения необходимой готовности.

При наличии необходимых ресурсов готовность системы к выполнению требований заинтересованных сторон по качеству и срокам обеспечивают на основе своевременного выявления значимых изменений в потребностях и требованиях заинтересованных сторон и использования эффективных технологий для их реализации в системе.

При экспоненциальной аппроксимации исходных характеристик и их независимости вероятность нарушения готовности системы к выполнению требований заинтересованных сторон по качеству и срокам $R_{кач}$ вычисляют по формулам:

- для случая, когда начало реализации в системе необходимых функциональных изменений (для удовлетворения изменившихся потребностей и требований заинтересованных сторон) наступает сразу после появления значимых изменений в потребностях и требованиях заинтересованных сторон:

$$R_{кач} = 1 - \frac{\xi^2}{q(\xi + T_{реализации})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right],$$

$$R_{кач} = 1 - \frac{\xi}{\xi + T_{реализация}}; \qquad (В.4)$$

- для случая периодической реализации в системе накопившихся значимых изменений в потребностях и требованиях заинтересованных сторон:

$$R_{кач} = 1 - \frac{\xi^2}{q(\xi + T_{реализации})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right]. \qquad (В.5)$$

где ξ — ожидаемое среднее время между значимыми изменениями в реальных потребностях и требованиях заинтересованных сторон. Значимые изменения требуют их реализации в системе (т. е. ξ^{-1} — виртуальная частота значимых изменений в потребностях и требованиях заинтересованных сторон);

$T_{реализации}$ — среднее время реализации накопившихся изменений в системе;

q — установленный или возможный период между соседними моментами начала реализации накапливаемых изменений потребностей и требований заинтересованных сторон в системе (т. е. q^{-1} — виртуальная частота реализации изменений для случая периодической реализации в системе накопившихся значимых изменений).

Для задаваемого периода прогноза $T_{зад}$ показатель удовлетворенности заинтересованных сторон по качеству и срокам, используемый в расчетах обобщенного риска в В.2.4, определяют следующим образом:

$$Z_{кач}(T_{зад}) = \begin{cases} 0, \text{ если требования заинтересованных сторон по качеству и срокам выполнены;} \\ R_{кач} \text{ по формулам (В.4), (В.5), если требования не выполнены или не заданы.} \end{cases} \qquad (В.6)$$

Условие по выполнению требований заинтересованных сторон по качеству и срокам определено для периода прогноза как условие непревышения максимально допустимого уровня риска $R_{доп\ кач}$, задаваемого для вероятности нарушения удовлетворенности заинтересованных сторон по качеству и срокам $R_{кач}$. Это условие выражается в форме $R_{кач} \le R_{доп\ кач}$.

В.2.3.3 Для оценки вероятности нарушения готовности системы к выполнению требований заинтересованных сторон по затратам и использования этой вероятности в расчетах обобщенного риска (см. В.4) применяют показатель удовлетворенности заинтересованных сторон по затратам $Z_{затрат}(T_{зад})$. Для его расчета и учета различий по затратам все условия заинтересованных сторон группируют по M типам ($m = 1, \ldots, M$, $M \ge 1$). К m-му типу относят $a_m \ge 1$ заинтересованных сторон, причем в пределах периода прогноза делают предположение, что каждому из типов свойственны свои приблизительно одинаковые затраты на разработку, ввод в эксплуатацию, эксплуатацию, сопровождение системы и ее выведение из эксплуатации (этот уровень затрат характеризует степень удовлетворенности заинтересованных сторон). Условия выполнения требований заинтересованных сторон m-го типа по затратам учитывают в виде индикаторной функции $Ind\ (\alpha) = Ind\ (C_m \le C_{доп\ m})$ — см. формулу (В.1), где $C_{доп\ m}$ — допустимые общие затраты заинтересованных сторон m-го типа системы относительно задаваемого периода прогноза $T_{зад}$ при эксплуатации системы При этом общие затраты заинтересованных сторон m-го типа системы $C_m(T_{зад})$ за период $T_{зад}$, соизмеримые со всем жизненным циклом системы для достижения целей процесса аттестации, оценивают по формуле

$$C_m(T_{зад}) = C_{разр\ m} + C_{ввод\ m} + C_{экспл\ m}(T_{зад}) + C_{сопр\ m}(T_{зад}) + C_{списан\ m}, \qquad (В.7)$$

где $C_{разр\ m}$ — затраты заинтересованных сторон m-го типа на разработку системы (ожидаемые или реальные);

$C_{ввод\ m}$ — затраты заинтересованных сторон m-го типа на ввод в эксплуатацию системы (ожидаемые или реальные);

$C_{экспл\ m}(T_{зад})$ — затраты заинтересованных сторон m-го типа на эксплуатацию системы за задаваемый период прогноза $T_{зад}$;

$C_{сопр\ m}(T_{зад})$ — затраты заинтересованных сторон m-го типа на сопровождение системы за задаваемый период прогноза $T_{зад}$;

$C_{\text{списан } m}$ — затраты заинтересованных сторон m-го типа на выведение системы из эксплуатации (ожидаемые или реальные).

Показатель удовлетворенности заинтересованных сторон по затратам $Z_{\text{затрат}}(T_{\text{зад}})$ определяют для задаваемого периода прогноза $T_{\text{зад}}$. Это время может накрывать только прошедший период (тогда учитывают реальные затраты) или может включать период прогноза на будущее вплоть до завершения жизненного цикла системы (в этом случае учитывают ожидаемые затраты). Показатель $Z_{\text{затрат}}(T_{\text{зад}})$ определяют следующим образом:

$$Z_{\text{затрат}}(T_{\text{зад}}) = \begin{cases} 0, & \text{если условия заинтересованных сторон по затратам выполнены;} \\ \delta_{\text{затрат}}(T_{\text{зад}}) \text{ по (В.9)}, & \text{если условия не выполнены или не заданы,} \end{cases} \quad \text{(В.8)}$$

где

$$\delta_{\text{затрат}}(T_{\text{зад}}) = \sum_{m=1}^{M} bhd\left(C_{m}(T_{\text{зад}}) \le C_{\text{доп } m}\right) \cdot a_{m} \Big/ \sum_{m=1}^{M} a_{m}. \quad \text{(В.9)}$$

Примечания

1 В частных случаях, определяемых моментом завершения периода прогноза, в формуле (В.7) оставляют лишь те составляющие, которые по времени входят в период прогноза $T_{\text{зад}}$. Например, если задаваемый период прогноза $T_{\text{зад}}$ накрывает стадии эксплуатации и сопровождения системы (как правило, именно такие периоды прогноза выбирают при системном анализе), то от длительности периода $T_{\text{зад}}$ зависят затраты лишь на этих стадиях. Для достижения целей аттестации системы затраты на других стадиях полагают неизменными.

2 При необходимости на уровне индикаторной функции дополнительно могут быть учтены иные условия и требования заинтересованных сторон к извлечению пользы от эксплуатации системы (социально-экономических благ, прибыли, обеспечения занятости населения, научно-технических достижений, предотвращения ущербов, обеспечения различных видов безопасности, иной пользы, как измеряемой, так и не измеряемой количественно).

В.2.4 Оценка обобщенного риска нарушения надежности реализации процесса аттестации системы

В.2.4.1 Общие положения

Обобщенный риск нарушения надежности реализации процесса аттестации системы без учета требований по защите информации оценивают с помощью расчетной вероятности невыполнения необходимых действий процесса аттестации (см. В.2.2) и показателей нарушения готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам (см. В.2.3).

При этом обобщенный показатель риска нарушения надежности реализации процесса без учета требований по защите информации характеризуется переходом в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: либо из-за невыполнения необходимых действий процесса, либо из-за нарушения готовности системы к выполнению требований заинтересованных сторон, либо из-за комбинации каких-либо перечисленных выше причин.

В.2.4.2 Метод оценки

Обобщенный риск нарушения надежности реализации процесса аттестации системы без учета требований по защите информации вычисляют по формуле

$$R_{\text{обобщен}}(T_{\text{зад}}) = 1 - [1 - Z_{\text{действий}}(T_{\text{зад}})] \cdot [1 - Z_{\text{кач}}(T_{\text{зад}})] \cdot [1 - Z_{\text{затрат}}(T_{\text{зад}})]. \quad \text{(В.10)}$$

Исходные данные и порядок расчетов определены в В.2.2, В.2.3.

Если все условия по выполнению необходимых действий процесса аттестации системы и обеспечению готовности системы к выполнению требований заинтересованных сторон соблюдены, то обобщенный риск нарушения надежности реализации процесса аттестации системы без учета требований по защите информации обращается в ноль (с интерпретацией: этим риском из-за его несущественности можно пренебречь).

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

В.3.1 Общие положения

В.3.1.1 Прогнозирование рисков нарушения требований по защите информации осуществляют на основе применения математических моделей для прогнозирования риска нарушения требований по защите информации, см. ГОСТ Р 59341—2021 (В.2 приложения В). Все положения по моделированию, изложенные в ГОСТ Р 59341 применительно к процессу управления информацией, в полной мере применимы к процессу аттестации системы (в части, свойственной прогнозированию риска нарушения требований по защите информации). Для расчета типовых показателей рисков анализируемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. В моделях и методах системного анализа применительно к таким моделируемым системам 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.

В.3.1.2 В моделях простой структуры под моделируемой системой понимается определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявлены требования и применяют меры защиты информации. 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. Система сложной структуры рассматривается как совокупность взаимодействующих элементов, каждый из которых представляется в виде «черного ящика», функционирующего в условиях неопределенности.

В.3.1.3 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 может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.3.1.4 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.

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. Такая интерпретация подразумевает выполнение требований по защите информации не только применительно к защищаемым активам и действиям, с помощью которых создают и получают выходные результаты, но и к самим выходным результатам, которые применяют (или планируют к созданию, получению и/или применению). В итоге для каждого из элементов и моделируемой системы в целом в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси образовано следующими двумя основными состояниями:

- «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.

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

В.3.1.5 В моделях простой структуры под моделируемой системой понимается определенное действие или выходной результат и совокупность задействованных активов, к которым предъявлены требования и осуществляются меры защиты информации. Такую систему рассматривают как «черный ящик», если для него сделано предположение об использовании одной и той же модели угроз 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 моделируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логически представляет собой определенное действие или выходной результат и совокупность задействованных активов, к которым предъявлены требования и применены меры защиты информации. При этом выходной результат сам может стать активом в итоге выполняемых действий.

В общем случае для различных элементов системы сложной структуры могут быть применены различные модели угроз безопасности информации или различные технологии системного контроля выполнения требований по защите информации и восстановления целостности системы.

В.3.1.6 При расчетах с использованием математических моделей для прогнозирования риска нарушения требований по защите информации и рекомендаций ГОСТ Р 59341—2021 (В.2, В.3 приложения В) осуществляется учет предпринимаемых мер периодической диагностики и восстановления возможностей по обеспечению выполнения требований по защите информации. В результате математического моделирования рассчитывают вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение

до единицы, представляющее собой вероятность нарушения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе нарушено»). В свою очередь вероятность нарушения требований по защите информации в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения требований по защите информации в процессе аттестации системы.

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 — «черного ящика», используют исходные данные, формально определяемые в общем случае следующим образом:

σ — частота возникновения источников угроз в процессе аттестации 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;

$T_{зад}$ — задаваемый период прогноза.

Расчетные показатели:

$P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ — вероятность отсутствия нарушений по защите информации в процессе аттестации системы в течение периода прогноза $T_{зад}$;

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

Расчет показателей применительно к процессу аттестации для моделируемой системы простой и сложной структуры осуществляют по формулам ГОСТ Р 59341—2021 (В.2 приложения В).

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 аттестации с учетом требований по защите информации

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

$$R_{интегр}(T_{зад}) = 1 - [1 - R_{обобщен}(T_{зад})] \cdot [1 - R_{наруш}(T_{зад})], \quad (В.11)$$

где $R_{обобщен}(T_{зад})$ — вероятность нарушения надежности реализации процесса аттестации 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 в процессе аттестации системы в течение периода прогноза $T_{зад}$, рассчитывается по моделям и рекомендациям В.3.

Вероятность нарушения надежности реализации процесса в течение периода прогноза без учета требований по защите информации $R_{обобщен}(T_{зад})$ рассчитывают по формуле (В.10) в зависимости от целей системного анализа. Вероятность нарушения требований по защите информации в системе в течение периода прогноза $R_{наруш}(T_{зад})$ рассчитывают по рекомендациям В.3 для выбранной структуры моделируемой системы.

Интегральный риск нарушения реализации процесса аттестации системы с учетом требований по защите информации определяют путем сопоставления расчетной интегральной вероятности нарушения реализации процесса в течение периода прогноза, рассчитанной по формуле (В.11), с возможным ущербом за этот период.

Примечание — Примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение Г
(справочное)

Типовые допустимые значения показателей рисков для процесса аттестации 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 аттестации 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 рассматриваемой системы, увеличивает время до принятия ее в эксплуатацию и удорожает саму эксплуатацию системы.

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

Типовые допустимые значения количественных показателей рисков для процесса аттестации системы отражены в таблице Г.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 аттестации системы в течение задаваемого периода прогноза.

Таблица Г.1 — Пример задания допустимых значений рисков

Показатель	Допустимое значение риска (в вероятностном выражении)	
	при ориентации на обоснование по прецедентному принципу	при ориентации на обоснование для системы-эталона
Риск нарушения требований по защите информации в процессе аттестации системы	Не выше 0,05	Не выше 0,01
Интегральный риск нарушения реализации процесса аттестации системы с учетом требований по защите информации	Не выше 0,1	Не выше 0,05

Приложение Д
(справочное)

Примерный перечень методик системного анализа для процесса аттестации системы

Д.1 Методика прогнозирования риска нарушения требований по защите информации в процессе аттестации системы.

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

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

Д.4 Методики выявления явных и скрытых недостатков процесса аттестации системы с использованием прогнозирования рисков.

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

Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам аттестации системы.

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

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

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

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

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

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

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

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

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

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

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

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

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

Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 11.05.2021. Подписано в печать 21.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.

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