ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59337— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОЦЕНКИ И КОНТРОЛЯ ПРОЕКТА

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»), Обществом с ограниченной ответственностью «Научно-исследовательский институт прикладной математики и сертификации» (ООО НИИПМС) и Акционерным обществом «Научно-производственное объединение «Эшелон» (АО «НПО Эшелон»)

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 28 апреля 2021 г. № 312-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, портфелем проектов, человеческими ресурсами, качеством, знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;

- для процессов технического управления — процессов планирования проекта, управления решениями, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343. Для оценки и контроля проекта — по настоящему стандарту;

- 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, сопровождения, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357.

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

Для планируемого и реализуемого процесса оценки и контроля проекта применение настоящего стандарта при создании (модернизации, развитии), эксплуатации и сопровождения систем обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОЦЕНКИ И КОНТРОЛЯ ПРОЕКТА

System engineering. Protection of information in project assessment and control process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные методические положения системного анализа для процесса оценки и контроля проекта применительно к вопросам защиты информации для систем различных областей приложения.

Для практического применения в приложениях А—Д приведены примеры перечней активов, подлежащих защите, и угроз, типовые модели и методы прогнозирования рисков, 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 оценки и контроля проекта, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем — см. примеры систем в [1]—[27].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

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

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

Издание официальное

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

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

ГОСТ Р ИСО 2859-1 Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 1. Планы выборочного контроля последовательных партий на основе приемлемого уровня качества

ГОСТ Р ИСО 2859-3 Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 3. Контроль с пропуском партий

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 10014 Менеджмент организации. Руководящие указания по достижению экономического эффекта в системе менеджмента качества

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/МЭК 15504-5 Информационные технологии. Оценка процессов. Часть 5. Образец модели оценки процессов жизненного цикла программного обеспечения

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

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

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 50779.41 Статистические методы. Контрольные карты для арифметического среднего с предупреждающими границами

ГОСТ Р 50779.70 Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Введение в стандарты серии ГОСТ Р ИСО 2859

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 Менеджмент риска. Термины и определения

ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.5 Менеджмент риска. Руководство по применению методов анализа надежности

ГОСТ Р 51901.7 Менеджмент риска. Руководство по внедрению ИСО 31000

ГОСТ Р 51901.16 Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки

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

ГОСТ Р 53622 Информационные технологии. Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов

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 оценке рисков. Общая методология

ГОСТ Р 54869—2011 Проектный менеджмент. Требования к управлению проектом

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

ГОСТ Р 57100 Системная и программная инженерия. Описание архитектуры

ГОСТ Р 57102 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288

ГОСТ Р 57193—2016 Системная и программная инженерия. Процессы жизненного цикла систем

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 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 50922, ГОСТ Р 51275, 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 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.2

жизненный цикл системы: Развитие системы, продукции, услуги, проекта или другой создаваемой человеком сущности от замысла до списания.

ГОСТ Р 57193—2016, пункт 4.1.19

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: 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: 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 оценки и контроля проекта с учетом требований по защите информации:** Сочетание вероятности того, что будут нарушены надежность реализации процесса оценки и контроля проекта либо требования по защите информации, либо и то и другое, с тяжестью возможного ущерба.

3.1.9

информационная инфраструктура: Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

[ГОСТ Р 53114—2008, статья 3.1.4]

3.1.10 **надежность реализации процесса оценки и контроля проекта с учетом требований по защите информации:** Свойство процесса оценки и контроля проекта сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса в заданных условиях реализации с соблюдением требований по защите информации.

3.1.11

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.12

обеспечивающая система: Система, которая служит дополнением к рассматриваемой системе на протяжении стадий ее жизненного цикла, но необязательно вносит непосредственный вклад в ее функционирование.

Примечания

1 Например, когда рассматриваемая система вступает в стадию производства, требуется обеспечивающая производственная система.

2 Каждая обеспечивающая система имеет свой собственный жизненный цикл. Настоящий стандарт может применяться для любой обеспечивающей системы, если она представляется в качестве рассматриваемой системы.

[ГОСТ Р 57193—2016, пункт 4.1.16]

3.1.13

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.14

проект: Комплекс взаимосвязанных мероприятий, направленный на создание уникального продукта или услуги в условиях временных и ресурсных ограничений.

[ГОСТ Р 54869—2011, пункт 3.12]

3.1.15 **проект-эталон:** Реальный или гипотетичный проект, который по своим показателям интегрального риска нарушения реализации рассматриваемого процесса оценки и контроля проекта с учетом требований по защите информации принимается в качестве эталона для полного удовлетворения требований заинтересованных сторон проекта и 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.

3.1.16

процесс: Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

[ГОСТ Р 57193—2016, пункт 4.1.26]

3.1.17 **рассматриваемая система:** Система, относительно которой в рамках настоящего стандарта применяется процесс оценки и контроля проекта.

3.1.18

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.19

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

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

3.1.21

стадия: Период в пределах жизненного цикла некоторой сущности, который относится к состоянию ее описания и реализации.

Примечания

1 В настоящем стандарте принято, что стадии относятся к основному развитию и достижению контрольных точек в течение жизненного цикла этой сущности.

2 Стадии могут быть взаимно пересекающимися.

[ГОСТ Р 57193—2016, пункт 4.1.41]

3.1.22

требование: Утверждение, которое отражает или выражает потребность и связанные с ней ограничения и условия.

Примечание — Требования существуют на различных уровнях и выражают потребность в высокоуровневой форме (например, требование компонента программного обеспечения).

[ГОСТ Р ИСО/МЭК 15026-1—2016, статья 3.2.5]

3.1.23

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

[ГОСТ Р 50922—2006, статья 2.9.2]

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

3.1.25

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

[ГОСТ Р 50922—2006, статья 2.9.1]

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

3.2 В настоящем стандарте использовано сокращение:

ТЗ — техническое задание.

4 Основные положения системной инженерии по защите информации в процессе оценки и контроля проекта

4.1 Общие положения

Организации используют данный процесс в рамках проекта, связанного с созданием (модернизацией, развитием), эксплуатацией и сопровождением системы для обеспечения ее безопасности и эффективности. Процесс оценки и контроля проекта осуществляют периодически или при наступлении важных событий для системного анализа результатов работы в соответствии с требованиями, планами и всевозможными бизнес-целями. Если в результате реализации процесса обнаруживают недопустимые риски, формируют необходимую информацию для реагирования на них.

В процессе оценки и контроля проекта осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

Для прогнозирования рисков нарушения надежности реализации процесса и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых преде-

лах используют системный анализ с учетом требований по защите информации в условиях возможных угроз надежности реализации процесса и безопасности информации.

Определение выходных результатов процесса оценки и контроля проекта 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 20000-1, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, [1]—[27] с учетом специфики проекта. Оценку интегрального риска нарушения реализации процесса оценки и контроля проекта осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51583, ГОСТ Р 51897, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355. При этом учитывают специфику организации, применяющей процесс, и самого проекта — см., например, [20]—[27].

4.2 Цели процесса и назначение мер по защите информации

4.2.1 Определение цели процесса оценки и контроля проекта осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО 10014, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 53647.1, ГОСТ Р 54869, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики организации, применяющей процесс.

В общем случае цель процесса оценки и контроля проекта состоит в определении, сопровождении и обеспечении гарантий наличия в организации необходимых политик, процессов, моделей, методик, инструментариев и процедур и в их результативном использовании в проекте.

4.2.2 Меры по защите информации в процессе оценки и контроля проекта предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер по защите информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [20]—[25] с учетом специфики планируемого проекта и организации, выполняющей проект.

4.3 Стадии и этапы жизненного цикла

В общем случае процесс оценки и контроля проекта задействован на всех стадиях и этапах жизненного цикла систем, создаваемых (модернизируемых, развиваемых) и эксплуатируемых организацией. Стадии и этапы работ по созданию (модернизации, развитию), эксплуатации и сопровождения систем, связанных с проектом, устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования систем, связанных с проектом. Перечень этапов и конкретных работ в жизненном цикле систем формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ Р 15.301, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 53622, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 59329. Процесс оценки и контроля проекта может входить в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости включать в себя другие процессы.

4.4 Основные принципы

При проведении системного анализа процесса оценки и контроля проекта руководствуются основными принципами, определенными в ГОСТ Р 59349, с учетом дифференциации требований по защите информации в зависимости от категории значимости проекта и важности информации, предполагаемой к обработке в рамках систем, связанных с этим проектом — см. ГОСТ Р 59346, [20]—[25]. Все применяемые принципы подчинены принципу целенаправленности осуществляемых действий.

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе оценки и контроля проекта 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 оценки и контроля проекта

5.1 Требования системной инженерии по защите информации устанавливают в соответствии с нормативами, положениями, политиками и процедурами, принятыми в организации, выполняющей этот процесс, с учетом нормативно-правовых документов Российской Федерации (см., например, [1]—[27]), уязвимостей самого процесса, преднамеренных и непреднамеренных угроз нарушения его реализации и безопасности информации, а также задействованных при его реализации программных и программно-аппаратных элементов — см. ГОСТ Р 59346. Поскольку процесс оценки и контроля проекта относится к категории процессов технического управления, применимые к нему требования к защите информации устанавливают в соответствии с принятыми в организации, выполняющей этот процесс, нормативами, положениями, политиками и процедурами.

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

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

Требования системной инженерии по защите информации в процессе оценки и контроля системы включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе оценки и контроля проекта определяют по ГОСТ 2.114, ГОСТ 7.32, ГОСТ 15.016, ГОСТ 15.101, ГОСТ Р 15.301, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики проекта и организации, применяющей процесс.

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 оценки и контроля проекта.

5.5 Определение активов, информация которых или о которых подлежит защите, формирование перечня потенциальных угроз надежности реализации процесса и безопасности информации 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 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62264-1, [20]—[25]. Примеры перечней учитываемых активов и угроз в процессе оценки и контроля проекта приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процесса оценки и контроля проекта анализируют по показателям рисков в зависимости от специфики системы, связанной с проектом, 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 2859-1, ГОСТ Р ИСО 2859-3, 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 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 15504-5, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, 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, [20]—[27].

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 оценки и контроля проекта определен в 6.3.

Типовые модели и методы системного анализа процесса оценки и контроля проекта, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д. Характеристики мер защиты информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют 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 планирования проекта, к которым предъявлены определенные требования по защите информации, осуществляют оценку эффективности защиты информации на основе прогнозирования рисков. Для обоснования эффективных предупреждающих действий по снижению риска или его удержанию в допустимых пределах используют системный анализ.

6.1.2 В общем случае основными выходными результатами процесса оценки и контроля проекта являются:

- показатели качества функционирования системы, связанной с проектом, или результаты их оценки;
- распределение ролей, ответственностей, подотчетности и полномочий персонала системы, связанной с проектом,;
- оценка ресурсов проекта;
- анализ продвижения проекта;
- результаты соответствия планов фактическому состоянию проекта,
- информированность заинтересованных сторон о состоянии проекта;
- корректирующие действия или решение о перепланировании;
- согласованность проектных действий, позволяющих продвигаться от одной запланированной контрольной точки или события к следующему;
- степень достижения целей проекта.

6.1.3. Для получения выходных результатов процесса оценки и контроля проекта в общем случае выполняют следующие основные действия:

- определение стратегии процесса, включая методы оценки, графики работ, необходимые управленческие решения и технический анализ;
- системный анализ достижения целей и реализации планов проекта;

- анализ управленческих и производственных планов для определения их результативности и выполнимости;
- сравнение плановой и фактической (на текущий момент) стоимости проекта, анализ сроков выполнения;
- оценку распределения ролей, ответственности, подотчетности и достаточности полномочий управленческого персонала;
- оценку адекватности и пригодности ресурсов, включая инфраструктуру, персонал, финансирование, время на выполнение работ;
- оценку выполнения проекта, включая сбор данных и оценку фактических и плановых затрат, наличие материалов, получение услуг, анализ других технических данных;
- организацию необходимого управления, анализа, аудита и инспекций;
- осуществление регулярных проверок критичных процессов и новых технологий, своевременную корректировку планов;
- анализ результатов проверок и подготовку рекомендаций по совершенствованию системы, связанной с проектом,
- документирование и обеспечение статуса результатов процесса оценки и контроля проекта;
- наблюдение за исполнением результатов и рекомендаций процесса оценки и контроля проекта;
- взаимодействие с приобретающей стороной или поставщиком при возникновении необходимости внесения изменений по стоимости, времени или качеству продукции для разрешения возможных проблем;
- санкционирование продвижения проекта к следующей контрольной точке или событию (если это обосновано).

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процесса оценки и контроля проекта, 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).

Примечание — Определение активов, действий и выходных результатов процесса оценки и контроля проекта в системах искусственного интеллекта происходит с учетом требований, указанных в примечании к 5.1.

6.2 Требования к составу показателей

Выбираемые показатели должны обеспечивать проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения реализации процесса оценки и контроля проекта 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 нарушения эффективности на ранних этапах проявления явных и скрытых угроз, когда можно принять предупреждающие корректирующие меры защиты информации. 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 В процессе оценки и контроля проекта для прогнозирования рисков с учетом нарушения требований по защите информации используют качественные и количественные показатели. Качественные показатели определяют по ГОСТ Р ИСО/МЭК 27005.

Для процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления и технических процессов (за исключением процесса определения системных требований) используют следующие количественные показатели:

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

Для технического процесса определения системных требований (по ГОСТ Р 59346) используют следующие количественные показатели:

- частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения функционирования системы);
- частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения требований по защите конфиденциальной информации в системе или о системе);
- интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований.

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

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

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессу оценки и контроля проекта):

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

7.1 Требования к системному анализу в процессе оценки и контроля проекта включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в процессе оценки и контроля проекта.

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

7.2 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 проекта и организации, применяющей процесс оценки и контроля проекта.

Примечание — Примеры решения задач системного анализа приведены в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе оценки и контроля проекта 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 [20]—[25];
- договоры и соглашения на проведение работ по созданию (модернизации, развитию) системы;
- лицензии, подтверждающие право поставщика (производителя) на проведение работ по созданию (модернизации, развитию) системы;
- финансовые и плановые документы, связанные с эксплуатацией системы, проведением работ по созданию (модернизации, развитию) системы;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101, с учетом специфики создаваемой (модернизируемой) и/или применяемой системы;
- конструкторскую и технологическую документацию (для модернизируемой или применяемой системы) — по ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201;
- эксплуатационную и ремонтную документацию — по ГОСТ Р 2.601, ГОСТ 2.602, ГОСТ 34.201 с учетом специфики создаваемой (модернизируемой) и/или применяемой системы;
- документацию системы менеджмента качества организации — по ГОСТ Р ИСО 9001;
- технические задания — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839, с учетом специфики создаваемой (модернизируемой) системы;
- персональные данные, базу данных и базу знаний, систему хранения архивов;
- систему передачи данных и облачные данные организации;
- выходные результаты иных процессов в жизненном цикле систем, относящихся к проекту, с учетом их специфики.

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе оценки и контроля проекта 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 [20]—[25];
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы — по ГОСТ Р ИСО/МЭК 27002 и ГОСТ Р 54124;
- угрозы безопасности информации при подготовке и обработке документов — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412;
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному приобретателю (заказчику), информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги;
- угрозы несанкционированного удаления защищаемой информации, несогласованности правил доступа к большим данным, преодоления физической защиты, приведения системы в состояние «отказ в обслуживании», утраты носителей информации, хищения средств хранения, обработки и (или) ввода/вывода/передачи информации, перехвата управления информационной системой;
- 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

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

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

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процессы приобретения и поставки продукции и услуг для системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59329—2021, приложение В
Процесс управления моделью жизненного цикла системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59330—2021, приложение В
Процесс управления инфраструктурой системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59331—2021, приложение В
Процесс управления портфелем проектов	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59332—2021, приложение В
Процесс управления человеческими ресурсами системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59333—2021, приложение В
Процесс управления качеством системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59334—2021, приложение В
Процесс управления знаниями о системе	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59335—2021, приложение В

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые методы и модели
Процесс планирования проекта	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59336—2021, приложение В
Процесс оценки и контроля проекта	По 6.3	Настоящий стандарт, приложение В
Процесс управления решениями	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59338—2021, приложение В
Процесс управления рисками для системы	По ГОСТ Р 59339—2021, пункт 6.3	ГОСТ Р 59339—2021, приложение В
Процесс управления конфигурацией системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59340—2021, приложение В
Процесс управления информацией системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59341—2021, приложение В
Процесс измерений системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59342—2021, приложение В
Процесс гарантии качества для системы	По ГОСТ Р 59343—2021, пункт 6.3	ГОСТ Р 59343—2021, приложение В
Процесс анализа бизнеса или назначения системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59344—2021, приложение В
Процесс определения потребностей и требований заинтересованной стороны для системы	а) риск нарушения надежности реализации процесса без учета требований по защите информации; б) риск нарушения требований по защите информации в процессе; в) интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59345—2021, приложение В

Продолжение таблицы В.1

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

Окончание таблицы В.1

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

Примечание — Другие возможные показатели, модели и методы оценки рисков — см. в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 58494, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

Приложение Г
(справочное)

Рекомендации по определению допустимых значений показателей рисков

С точки зрения остаточного риска, характеризующего приемлемый уровень целостности рассматриваемого проекта, предъявляемые требования системной инженерии подразделяют на требования при допустимых рисках, обосновываемых по прецедентному принципу согласно ГОСТ Р 59349, и требования при рисках, свойственных реальному или гипотетичному проекту-эталону. При формировании требований системной инженерии необходимо обоснование достижимости целей проекта и рассматриваемого процесса оценки и контроля проекта, 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 проекта, ограничения на условия его реализации, указывают другие условия в зависимости от специфики проекта и организаций, его выполняющих.

Требования системной инженерии при принимаемых рисках, свойственных проекту-эталону, являются наиболее жесткими, они не учитывают специфики рассматриваемых проекта, а ориентируются лишь на мировые технические и технологические достижения для удовлетворения требований заинтересованных сторон и рационального решения задач системного анализа. Полной проверке на соответствие этим требованиям подлежат проект и связанные с ним системы, составляющие их подсистемы и реализуемые процессы жизненного цикла. Выполнение этих требований является гарантией обеспечения высокого качества и безопасности рассматриваемого проекта. Вместе с тем проведение работ системной инженерии с ориентацией на риски, свойственные проекту-эталону, характеризуются существенно большими затратами по сравнению с требованиями, ориентируемыми на допустимые риски, обосновываемые по прецедентному принципу. Это заведомо удорожает проекты, увеличивает время до их завершения и принятия в эксплуатацию связанных с этими проектами систем.

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

Типовые допустимые значения количественных показателей рисков для процесса оценки и контроля проекта 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 качественной и безопасной реализации рассматриваемого процесса в течение задаваемого периода прогноза.

Таблица Г.1 — Ссылки для определения допустимых значений рисков в системных процессах

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

Окончание таблицы Г.1

Системный процесс	Ссылки на стандарты для определения допустимых значений рисков при ориентации на обоснование по прецедентному принципу и по проекту-эталону (или системе-эталону)
Процесс управления рисками для системы	ГОСТ Р 59339—2021, приложение Г
Процесс управления конфигурацией системы	ГОСТ Р 59340—2021, приложение Г
Процесс управления информацией системы	ГОСТ Р 59341—2021, приложение Д
Процесс измерений системы	ГОСТ Р 59342—2021, приложение Г
Процесс гарантии качества для системы	ГОСТ Р 59343—2021, приложение Д
Процесс анализа бизнеса или назначения системы	ГОСТ Р 59344—2021, приложение Г
Процесс определения потребностей и требований заинтересованной стороны для системы	ГОСТ Р 59345—2021, приложение Д
Процесс определения системных требований	ГОСТ Р 59346—2021, приложение Е
Процесс определения архитектуры системы	ГОСТ Р 59347—2021, приложение Д
Процесс определения проекта	ГОСТ Р 59348—2021, приложение Г
Процесс системного анализа	ГОСТ Р 59349—2021, приложение Д
Процесс реализации системы	ГОСТ Р 59350—2021, приложение Г
Процесс комплексирования системы	ГОСТ Р 59351—2021, приложение Г
Процесс верификации системы	ГОСТ Р 59352—2021, приложение Г
Процесс передачи системы	ГОСТ Р 59353—2021, приложение Г
Процесс аттестации системы	ГОСТ Р 59354—2021, приложение Г
Процесс функционирования системы	ГОСТ Р 59355—2021, приложение Д
Процесс сопровождения системы	ГОСТ Р 59356—2021, приложение Д
Процесс изъятия и списания системы	ГОСТ Р 59357—2021, приложение Г

Приложение Д
(справочное)

Рекомендации по перечню методик системного анализа для процесса оценки и контроля проекта

Ссылочные рекомендации по перечню методик системного анализа для процесса оценки и контроля проекта отражены в таблице Д.1.

Таблица Д.1 — Ссылки по перечню методик системного анализа

Системный процесс	Ссылки на стандарты по перечню методик системного анализа
Процессы приобретения и поставки продукции и услуг для системы	ГОСТ Р 59329—2021, Приложение Д
Процесс управления моделью жизненного цикла системы	ГОСТ Р 59330—2021, Приложение Д
Процесс управления инфраструктурой системы	ГОСТ Р 59331—2021, Приложение Е
Процесс управления портфелем проектов	ГОСТ Р 59332—2021, Приложение Д
Процесс управления человеческими ресурсами системы	ГОСТ Р 59333—2021, Приложение Е
Процесс управления качеством системы	ГОСТ Р 59334—2021, Приложение Д
Процесс управления знаниями о системе	ГОСТ Р 59335—2021, Приложение Е
Процесс планирования проекта	ГОСТ Р 59336—2021, Приложение Д
Процесс оценки и контроля проекта	Настоящий стандарт
Процесс управления решениями	ГОСТ Р 59338—2021, Приложение Е
Процесс управления рисками для системы	ГОСТ Р 59339—2021, Приложение Е
Процесс управления конфигурацией системы	ГОСТ Р 59340—2021, Приложение Д
Процесс управления информацией системы	ГОСТ Р 59341—2021, Приложение Е
Процесс измерений системы	ГОСТ Р 59342—2021, Приложение Д
Процесс гарантии качества для системы	ГОСТ Р 59343—2021, Приложение Е
Процесс анализа бизнеса или назначения системы	ГОСТ Р 59344—2021, Приложение Д
Процесс определения потребностей и требований заинтересованной стороны для системы	ГОСТ Р 59345—2021, Приложение Е
Процесс определения системных требований	ГОСТ Р 59346—2021, Приложение Ж
Процесс определения архитектуры системы	ГОСТ Р 59347—2021, Приложение Е
Процесс определения проекта	ГОСТ Р 59348—2021, Приложение Д
Процесс системного анализа	ГОСТ Р 59349—2021, Приложение Е
Процесс реализации системы	ГОСТ Р 59350—2021, Приложение Д
Процесс комплексирования системы	ГОСТ Р 59351—2021, Приложение Д
Процесс верификации системы	ГОСТ Р 59352—2021, Приложение Д
Процесс передачи системы	ГОСТ Р 59353—2021, Приложение Д
Процесс аттестации системы	ГОСТ Р 59354—2021, Приложение Д
Процесс функционирования системы	ГОСТ Р 59355—2021, Приложение Е

Окончание таблицы Д.1

Системный процесс	Ссылки на стандарты по перечню методик системного анализа
Процесс сопровождения системы	ГОСТ Р 59356—2021, Приложение Е
Процесс изъятия и списания системы	ГОСТ Р 59357—2021, Приложение Д

Примечания

1 Системной основой для создания методик служат положения разделов 5—7, рекомендации по методам, моделям и допустимым рискам из приложений В, Г, Д.

2 С учетом специфики системы допускается использование других научно обоснованных методов, моделей и 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 2007г. № 16-ФЗ «О транспортной безопасности»

[9] Федеральный закон от 22 июля 2008г. № 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] Р 50.1.094—2014 Менеджмент риска. Идентификация, оценка и обработка риска проекта на прединвестиционном, инвестиционном и эксплуатационном этапах

[20] 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)

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

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

[23] 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)

[24] 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)

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

[26] 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)

[27] 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, информация, модель, оценка и контроль проекта, риск, система, системная инженерия, управление

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 29.04.2021. Подписано в печать 19.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,20.

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