ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59338— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ РЕШЕНИЯМИ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 апреля 2021 г. № 313-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе управления решениями 7
5 Общие требования системной инженерии по защите информации в процессе управления решениями 8
6 Специальные требования к количественным показателям 10
7 Требования к системному анализу 12
Приложение А (справочное) Пример перечня защищаемых активов 13
Приложение Б (справочное) Пример перечня угроз 14
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 15
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса управления решениями 24
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса управления решениями 37
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса управления решениями 38
Библиография 39

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, 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, оценки и контроля проекта, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343. Для процесса управления решениями — 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 управления решениями и специальные требования к используемым количественным показателям.

Для планируемого и реализуемого процесса управления решениями применение настоящего стандарта при создании (модернизации, развитии), эксплуатации систем и выведении их из эксплуатации обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ РЕШЕНИЯМИ

System engineering.
Protection of information in decision management process

Дата введения — 2021—11—30

1 Область применения

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

Для практического применения в приложениях А—Е приведены примеры перечней активов, подлежащих защите, и угроз, типовые методы, модели и методические указания по прогнозированию рисков, типовые допустимые значения для показателей рисков и 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), эксплуатации систем, выведении их из эксплуатации и реализующими процесс управления решениями, 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 27.003 Надежность в технике. Состав и общие правила задания требований по надежности

Издание официальное

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

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 27.403 Надежность в технике. Планы испытаний для контроля вероятности безотказной работы

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

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

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

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

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

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

ГОСТ Р 58494—2019 Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

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

ГОСТ Р 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—2014 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 27.003, ГОСТ Р 27.403, ГОСТ 34.003, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 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

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]

3.1.3

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]

3.1.4

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]

3.1.5

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]

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

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

3.1.8

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.9

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.10 **принятие решения в режиме реального времени:** Принятие решения по реализации предупреждающих действий или возможного решения об осознанном бездействии в сложившихся условиях за такое время, в течение которого выполнение этих предупреждающих действий является практически осуществимым и обоснованно целесообразным.

3.1.11

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

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

3.1.13

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]

3.1.14

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]

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

3.1.16

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.

4 Основные положения системной инженерии по защите информации в процессе управления решениями

4.1 Общие положения

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

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

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

Определение выходных результатов процесса управления решениями 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 27003, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Определение интегрального риска с учетом требований по защите информации в процессе управления решениями осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р 27.403, ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, 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 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355. При этом учитывают специфику системы (см., например, [20]—[26]) и организации, применяющей процесс.

4.2 Стадии и этапы жизненного цикла системы

Процесс управления решениями может быть использован на любой стадии жизненного цикла системы. 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 системы формируют с учетом рекомендаций ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301,

ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839. Процесс управления решениями 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 управления решениями 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 системы.

В общем случае главная цель процесса управления решениями состоит в обеспечении аналитической основы для определения, характеристики и оценки множества альтернативных решений, выбора наиболее предпочтительных решений и направлений действий на любом этапе жизненного цикла системы.

4.3.2 Меры защиты информации в процессе управления решениями 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 МЭК 61508-7, [20]—[24] с учетом специфики системы и реализуемой стадии жизненного цикла.

4.4 Основные принципы

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

4.5 Основные усилия для обеспечения защиты информации

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

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

5 Общие требования системной инженерии по защите информации в процессе управления решениями

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы, ТЗ на приобретение и поставку продукции и/или услуг для 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 формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например [1]—[26]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

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

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

При использовании процесса управления решениями в системах искусственного интеллекта необходимо гарантированно подтверждать достаточность автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации), учитывать возможность повышения уровня конфиденциальности данных в процессе их обработки в системе искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации), регламентировать вопросы обеспечения конфиденциальности тестовых выборок исходных данных, используемых испытательными лабораториями при оценке соответствия прикладных систем искусственного интеллекта, с сохранением прозрачности и подотчетности этого процесса.

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

Требования системной инженерии по защите информации в процессе управления решениями включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе управления решениями определяют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики системы.

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

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

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.602, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом рекомендаций ГОСТ 15.016, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6 и специфики системы (см., например [20]—[26]).

Примеры перечней учитываемых активов и угроз в процессе управления решениями приведены в приложениях А и Б.

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

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 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 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, [21]—[26].

5.7 Для обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах применяют системный анализ с использованием устанавливаемых специальных качественных и количественных показателей рисков.

Качественные показатели для оценки рисков в области информационной безопасности определены в ГОСТ Р ИСО/МЭК 27005. Целесообразность использования количественных показателей рисков

в дополнение к качественным показателям может потребовать дополнительного обоснования. Состав специальных количественных показателей рисков в интересах системного анализа процесса управления решениями определен в 6.3.

Типовые модели и методы системного анализа процесса управления решениями, методические указания по прогнозированию рисков, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В—Е. Характеристики мер и действий по защите информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам и возможным условиям их реализации.

6 Специальные требования к количественным показателям

6.1 Общие положения

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

6.1.2 В общем случае основными выходными результатами процесса управления решениями являются:

- варианты решений, требующих альтернативного системного анализа;
- альтернативные направления действий;
- предпочтительные решения и направления действий;
- задокументированные обоснования решений и принятые при обоснованиях предположения и допущения.

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

- планирование управления решениями, включая:
  - разработку стратегии управления решением, в т. ч. определение ролей, обязанностей, подотчетности и полномочий, установление приоритетов, формирование принципов формализации, математического моделирования и отношения к результатам аналитических решений,
  - определение обстоятельств и потребностей в решении, включая формулирование проблем, неблагоприятных тенденций и открывающихся возможностей,
  - вовлечение соответствующих заинтересованных сторон в процесс принятия решений, использование их опыта и знаний;
- сбор, обработку и анализ информации для принятия решений, включая:
  - сбор и обработку необходимых данных, системный анализ их качества с использованием процесса управления информацией (см. 6.4 и ГОСТ Р 59341),
  - обоснование и выбор оцениваемых показателей и критериев принятия решений, выбор и/или разработку методик системного анализа для процесса управления решениями (см. 6.2, 6.3 и приложение Е),
  - определение области компромиссов и ограничений, обоснование допустимых значений показателей, характеризующих приемлемые решения, формирование альтернативных вариантов решений для системного анализа (см. раздел 7),
  - проведение системного анализа альтернативных вариантов решений и возможных направлений действий с использованием процесса системного анализа (см. раздел 7 и ГОСТ Р 59349);
- принятие решений и управление решениями, включая:
  - решение формализованных оптимизационных задач для альтернативных вариантов,
  - определение предпочтительных альтернатив по результатам системного анализа с использованием установленных критериев, обоснование и принятие приемлемого решения (в том числе в режиме реального времени) и рациональных направлений действий,
  - документирование отчетов по решению, отслеживание принятых ранее решений, в том числе оценку эффективности разрешения проблем, исправление неблагоприятных тенденций и обращение возможностей в преимущества.

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

Примечание — Определение активов, действий и выходных результатов процесса управления решениями 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 управления решениями 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 предпринять предупреждающие корректирующие действия. Дополнительно могут быть использованы вспомогательные статистические данные, характеризующие события, которые произошли, и их потенциальное влияние на эффективность защиты информации при реализации процесса. Эти данные позволяют исследовать произошедшие события и их последствия и сравнить 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 используют следующие количественные показатели:

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

6.3.2 Риск нарушения надежности реализации процесса управления решениями без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса (без учета требований по защите информации) в сопоставлении с возможным ущербом.

6.3.3 Риск нарушения требований по защите информации в процессе управления решениями 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 управления решениями 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 сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

- 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 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 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 управления решениями включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в жизненном цикле 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 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, 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 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 системы (см., например, [21]—[26]).

Примечание — Примеры решения задач системного анализа приведены в приложении Г, а также см. в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

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

- выходные результаты процесса — по 6.1.2;
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации — см., например [21]—[24];
- договоры и соглашения на проведение работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- лицензии, подтверждающие право поставщика (производителя) на проведение работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- финансовые и плановые документы, связанные с эксплуатацией системы, проведением работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101 с учетом специфики системы;
- конструкторскую и технологическую документацию (для модернизируемой или применяемой системы) — по ГОСТ 2.051, ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201;
- эксплуатационную и ремонтную документацию — по ГОСТ 2.602, ГОСТ 34.201, ГОСТ Р 2.601 с учетом специфики системы;
- документацию системы менеджмента качества организации — по ГОСТ Р ИСО 9001;
- технические задания — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839 с учетом специфики системы;
- персональные данные, базу данных и базу знаний, систему хранения архивов;
- систему передачи данных и облачные данные организации;
- выходные результаты иных процессов в жизненном цикле системы с учетом ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

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

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

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Основные положения

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

- риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации (см. В.1.2—В.1.9, В.2);
- риска нарушения требований по защите информации в процессе управления решениями (см. В.3);
- интегрального риска нарушения реализации процесса управления решениями с учетом требований по защите информации (см. В.4).

В.1.2 Для расчета типовых показателей рисков исследуемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. Под моделируемой системой понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения. Модели и методы прогнозирования рисков в таких системах 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, а также возможные гипотетичные данные.

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

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

В.1.4 Для математической формализации используют следующие основные положения:

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

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

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

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

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

В.1.8 Изложение моделей в В.2 дано в контексте нарушения надежности реализации процесса управления решениями без учета требований по защите информации, в В.3 приведены способы прогнозирования риска нарушения требований по защите информации в процессе (в том числе с использованием моделей В.2). Методы прогнозирования интегрального риска нарушения реализации процесса управления решениями с учетом требований по защите информации представлены в В.4. При этом интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации и риска нарушения требований по защите информации в этом процессе.

В приложении Г изложены методические указания по прогнозированию рисков для процесса управления решениями.

В.1.9 Другие возможные подходы для оценки рисков описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59349, ГОСТ Р 59356, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

В.2 Математические модели для прогнозирования риска нарушения надежности реализации процесса управления решениями

В.2.1 Общие положения

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

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

В.2.1.2 Для каждого элемента моделируемой системы возможны либо отсутствие какого-либо контроля, либо периодический системный контроль (диагностика) его целостности с необходимым восстановлением по результатам контроля.

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

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

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

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

Примечание — Обеспечение требуемого качества используемой для принятия решения информации предполагает надежное и своевременное представление полной, достоверной и, при необходимости, конфиденциальной информации в ходе ее сбора и обработки — по ГОСТ Р 59341.

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

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

Модель представляет собой частный случай модели В.2.3, если период между диагностиками состояния моделируемой системы больше периода прогноза. Учитывая это, используют формулы (В.1)—(В.3).

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

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

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

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

В рамках модели развитие событий в системе считается не нарушающим надежность реализации процесса управления решениями в течение заданного периода прогноза (см. также В.2.4), если в течение всего периода прогноза источники угроз отсутствуют либо за время между соседними диагностиками возникшие источники угроз не успевают активизироваться. При этом в модели предполагается, что при очередном контроле (диагностике) происходит своевременное выявление каждого источника угроз и принятие адекватных защитных мер и действий против активизации выявленных угроз (см. иллюстрирующие примеры угроз, меры и действия по противодействию угрозам в Г.7).

В целях моделирования предполагают, что существуют не только средства контроля (диагностики) состояния моделируемой системы (позволяющие выявить источники угроз и следы их активизации), но и способы поддержания и/или восстановления нарушаемых возможностей системы. Восстановление осуществляется лишь в период системного контроля (диагностики) или сразу после него при выявлении источников угроз или следов их активизации. Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии обеспечения надежности реализации рассматриваемого процесса в период прогноза (т. к. в принятой модели за счет предупреждающих действий по результатам диагностики устраняются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент нанесения ущерба от реализации какой-либо угрозы).

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

Примечание — Если активизация угрозы мгновенная, это считают эквивалентным внезапному отказу. Усилия системной инженерии как раз и направлены на использование времени постепенной активизации угроз для своевременного выявления, распознавания и противодействия им.

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

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

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

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса, выходных результатов и/или защищаемых активов) с точки зрения нарушения надежности реализации процесса;

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

$T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы (без использования метода повышения адекватности модели по В.2.4 действует ограничительное допущение, что среднее время восстановления нарушаемой целостности системы, выявляемой при диагностике, включено в среднее время системной диагностики);

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы (используется в случае применения метода повышения адекватности модели по В.2.4);

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

Примечание — Примеры переопределения этих исходных данных (согласно В.2.4), конкретизированные в приложении к выходным результатам и действиям процесса, приведены в Г.7.

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

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

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

Возможны два варианта:

- вариант 1 — заданный период прогноза $T_{зад}$ меньше периода между окончаниями соседних контролей целостности моделируемой системы ($T_{зад} < T_{меж} + T_{диаг}$);

- вариант 2 — заданный период прогноза $T_{зад}$ больше или равен периоду между окончаниями соседних контролей целостности моделируемой системы ($T_{зад} \geq T_{меж} + T_{диаг}$), т. е. за это время заведомо произойдет один или более контролей системы с восстановлением нарушенной целостности (если нарушения имели место).

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

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

Примечание — Эту же формулу используют для оценки риска отсутствия нарушений надежности реализации процесса управления решениями при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по математической модели «черного ящика» при отсутствии какого-либо контроля в В.2.2.

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

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

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

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

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

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

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

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

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

Формула (В.3) логически интерпретируется так: для обеспечения выполнения требований целостности моделируемой системы за весь период прогноза требуется обеспечение ее целостности на каждом из участков — будь то середина или конец задаваемого периода прогноза $T_{зад}$.

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

В итоге вероятность отсутствия нарушений надежности реализации процесса управления решениями в течение периода прогноза $T_{зад}$ определяется аналитическими выражениями (В.2)—(В.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (В.1) вероятность нарушения надежности реализации процесса управления решениями $R_{надежн}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по обеспечению реализации процесса. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения надежности реализации процесса управления решениями в течение заданного периода прогноза при использовании технологии периодического системного контроля.

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

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

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

Расчет основан на применении следующих инженерных способов.

1-й способ позволяет использовать одни и те же модели для расчетов различных показателей по области их приложения. Поскольку модели математические, то путем смыслового переопределения исходных данных возможно использование одних и тех же моделей для оценки показателей, различающихся по смыслу, но идентичных по методу их расчета. Применение этого способа позволяет соизмерять прогнозируемые риски для разнородных угроз по единой вероятностной шкале от 0 до 1.

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



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

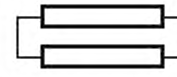


Рисунок В.2 — Система из параллельно соединенных элементов («ИЛИ»)

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

1) для системы из двух последовательно соединенных элементов

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

2) для системы из двух параллельно соединенных элементов

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

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

Рекурсивное применение соотношений (В.6), (В.7) снизу-вверх дает соответствующие вероятностные оценки для сложной логической структуры с параллельно-последовательным логическим соединением элементов.

Примечание — Способ рекурсивного применения процессов рекомендован ГОСТ Р 57102. Рекурсивное применение снизу-вверх означает первичное применение моделей В.2.2 или В.2.3 сначала для отдельных системных элементов, представляемых в виде «черного ящика» в принятой сложной логической структуре системы, затем, учитывая характер логического объединения («И» или «ИЛИ») в принятой структуре, по формулам (В.6) или (В.7) проводится расчет вероятности нарушения надежности реализации процесса за время t для объединяемых элементов (в принятых условиях независимости распределений их временных характеристик). И так — до объединения элементов на уровне сложной системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (В.6) или (В.7) от исходных параметров моделей В.2.1 и В.2.2.

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.2.2 и В.2.3 и применения 2-го способа получается вероятность нарушения надежности реализации процесса в течение заданного периода времени t. Если для каждого элемента просчитать эту вероятность для всех точек t от нуля до бесконечности, получится траектория функции распределения времени нарушения надежности реализации процесса по каждому из элементов в зависимости от реализуемых мер контроля и восстановления целостности, т. е. то, что используется в формулах (В.6) и (В.7). Полученный вид этой функции распределения, построенной по точкам (например, с использованием программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения надежности реализации процесса каждого из элементов и системы в целом. С точки зрения системной инженерии это среднее время интерпретируют как виртуальную среднюю наработку на нарушение надежности реализации процесса управления решениями при прогнозировании риска по моделям В.2.2 и В.2.3 для систем простой и сложной структуры. Обратная величина этого среднего времени является частотой нарушений надежности реализации процесса в условиях определенных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения процесса для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей В.2.2 и В.2.3 или аналогичных им для расчетов по моделям «черного ящика». Этот способ используют, когда изначальная статистика для определения частоты отсутствует или ее недостаточно.

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

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

$$T^{(2)}_{\text{диаг}} = T^{(1)}_{\text{диаг}} \cdot (1 - R^{(1)}) + R^{(1)} \cdot T_{\text{восст}}, \quad \text{(В.8)}$$

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

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

$$T^{(r)}_{\text{диаг}} = T^{(r-1)}_{\text{диаг}} \cdot (1 - R^{(r-1)}) + R^{(r-1)} \cdot T_{\text{восст}}, \quad \text{(В.9)}$$

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

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

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

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

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

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

Примечание — Способ итеративного применения процессов рекомендован ГОСТ Р 57102, применен в ГОСТ Р 58494.

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

В.2.5 Учет качества используемой информации

В случае критичности качества информации, используемой для принятия решений, действие сбора и анализа качества информации рассматривают отдельно. При этом дополнительно применяют модели и методы оценки качества выходной информации по ГОСТ Р 59341. В сопоставлении с возможным ущербом итоговый риск нарушения надежности реализации процесса управления решениями $R_{\text{надежн}}(T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации вычисляют по формуле

$$R_{\text{надежн}}(T_{\text{зад}}) = 1 - [1 - R_{\text{надежн. В.2.2-В.2.3}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш. УИ}}(T_{\text{зад}})], \quad \text{(В.10)}$$

где $R_{\text{надежн В.2.2-В.2.3}}(T_{\text{зад}})$ — вероятность нарушения надежности реализации процесса управления решениями в течение периода прогноза $T_{\text{зад}}$ без учета качества используемой информации и требований по защите информации, вычисляют по моделям и рекомендациям В.2.2, В.2.3;

$R_{\text{наруш. УИ}}(T_{\text{зад}})$ — вероятность нарушения надежности реализации процесса управления информацией в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации, вычисляют с помощью моделей и рекомендаций ГОСТ Р 59341—2021 (В.3.2—В.3.8, В.3.10 приложения В).

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

В.3.1 Общие положения

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

В моделях простой структуры под анализируемой системой понимают определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявлены требования и применяются меры защиты информации. Такую систему рассматривают как «черный ящик», если для него сделано предположение об использовании одной и той же модели угроз безопасности информации и одной и той же технологии системного контроля выполнения требований по защите информации и восстановления системы после состоявшихся нарушений или выявленных предпосылок к нарушениям. В моделях сложной структуры под моделируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логически представляет собой выходной результат или действие и совокупность задействованных активов (выходной результат становится активом в итоге выполняемых действий), к которым предъявлены требования и применяют меры защиты информации. В общем случае для системы сложной структуры для различных элементов могут быть применены различные модели угроз или различные технологии системного контроля выполнения требований по защите информации и восстановления системы. Отдельный элемент рассматривается как «черный ящик».

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

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

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

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

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

В.3.2 Исходные данные и расчетные показатели

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

σ — частота возникновения источников угроз нарушения требований по защите информации в процессе управления решениями;

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 моделируемой системе;

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

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

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

Расчетные показатели:

$P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ — вероятность отсутствия нарушений по защите информации в моделируемой системе 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 моделируемой системе в течение периода прогноза $T_{зад}$ в вероятностном выражении характеризует риск нарушения требований по защите информации в процессе управления решениями).

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

ущерба расчет риска нарушения требований по защите информации в процессе управления решениями в течение периода прогноза $R_{наруш}(T_{зад}) = R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ осуществляют как дополнение до единицы значения $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$.

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

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

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

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

где $R_{надежн}(T_{зад})$ — риск нарушения надежности реализации процесса управления решениями в течение периода прогноза $T_{зад}$ без учета требований по защите информации, в сопоставлении с возможным ущербом вычисляют по моделям и рекомендациям В.2;

$R_{наруш}(T_{зад})$ — риск нарушения требований по защите информации в процессе управления решениями в течение периода прогноза $T_{зад}$, в сопоставлении с возможным ущербом вычисляют по моделям и рекомендациям В.3.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса управления решениями

Г.1 Анализируемые объекты

Настоящие методические указания определяют типовые действия при расчетах основных количественных показателей рисков в процессе управления решениями:

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

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

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

Применительно к конкретной системе в целях прогнозирования рисков нарушения требований по защите информации для процесса управления решениями согласно 5.3, 6.1 определению подлежат:

- состав выходных результатов и выполняемых действий процесса управления решениями и используемых при этом активов;
- перечень потенциальных угроз и возможных сценариев возникновения и развития угроз для выходных результатов и выполняемых действий процесса управления решениями;
- иные сущности, используемые в прогнозировании рисков, при необходимости оценки того, насколько организация способна обеспечить возможности по выполнению процесса управления решениями в заданных условиях.

Примечание — Для понимания деталей специфики прогнозирования рисков см., например, ГОСТ Р 58494, где в приложении к системе дистанционного контроля в опасном производстве указаны примеры объектов, выходных результатов, выполняемых действий, множества потенциальных угроз.

Г.2 Цель прогнозирования рисков

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

Г.3 Положения по формализации

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

Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи (см. раздел 7). В общем случае моделируемую систему представляют либо в виде «черного ящика» (см. В.2.2 и В.2.3), либо в виде сложной структуры, элементы которой соединяются последовательно или параллельно (см. В.2.4).

Для получения более точных результатов прогнозирования рисков осуществляют декомпозицию сложной моделируемой системы до уровня составных системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых для описания целостности моделируемой системы логическими условиями «И» и «ИЛИ». При этом целостность моделируемой системы (системного элемента) в течение задаваемого периода прогноза означает такое состояние этой системы (системного элемента), которое в течение периода прогноза обеспечивает ее целевое назначение.

Примечания

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

2 Логическое условие «ИЛИ» для двух связанных этим условием элементов интерпретируется так: система из двух параллельно соединяемых элементов находится в состоянии целостности, когда первый элемент, второй

элемент «ИЛИ» находятся в состоянии целостности (в частности, когда для повышения надежности дублируется выполнение отдельных действий).

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

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

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

В приложении к прогнозированию интегрального риска нарушения реализации процесса относительно выполняемых действий с учетом требований по защите информации пространство элементарных состояний на временной оси может быть формально определено другими двумя основными состояниями:

- «Отсутствуют нарушения реализации процесса управления решениями», если в течение всего периода прогноза обеспечены «И» выполнение определенных действий процесса, «И» выполнение определенных требований по защите информации;
- «Реализация процесса управления решениями нарушена» — в противном случае, т. е. если в течение всего периода прогноза произошло хотя бы одно нарушение выполнения определенных действий процесса (например, с точки зрения безопасности, качества или эффективности системы, что должно быть заранее формально определено для практической интерпретации реальных нарушений при принятии решений) «ИЛИ» были нарушены определенные требования по защите информации, что может повлечь за собой возникновение недопустимого ущерба.

В общем случае с применением 1-го способа из В.2.4 возможно расширение или переименование самих элементарных состояний. Главное, чтобы они не пересекались (для однозначной интерпретации событий) и формировали полное множество элементарных состояний.

В Г.7 приведены примеры прогнозирования рисков.

Использование аппарата прогнозирования рисков позволяет обосновывать допустимые риски. По существу для каждого анализируемого объекта существуют свои условия приемлемости при использовании по назначению, что делает возможным выбор критерия допустимости риска, основанного на прецедентном принципе согласно приложению Д и ГОСТ Р 59349.

В качестве мер противодействия угрозам, способных снизить расчетные риски, могут выступать более частая (по сравнению со временем развития угроз) системная диагностика с восстановлением нормального функционирования моделируемой системы. При использовании задаваемых количественных границ допустимого риска статистические данные по реальным случаям нарушений этих границ позволяют формировать исходные данные для моделирования и осуществлять аналитическое обоснование упреждающих мер по снижению рисков или удержанию рисков в допустимых пределах и/или по снижению затрат и/или возможных ущербов при задаваемых ограничениях. Обоснованное определение сбалансированных системных мер, предупреждающих возникновение ущербов при ограничениях на ресурсы и допустимые риски, а также оценка и обоснование эффективных кратко-, средне- и долгосрочных планов по обеспечению безопасности осуществляют путем решения самостоятельных оптимизационных задач, использующих расчетные значения прогнозируемых рисков (см. рекомендуемый перечень методик в приложении Е).

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

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

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

Г.4 Показатели, исходные данные и расчетные соотношения

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

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

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

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

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

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

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

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

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

Шаг 4. Выбирают расчетные показатели. Выбирают подходящие математические модели и методы повышения их адекватности из В.2, В.3, В.4. Разрабатывают необходимые методики системного анализа, обеспечивающие более детальный учет особенностей процесса управления решениями (см. приложение Е). Осуществляют расчет выбранных показателей с использованием соотношений (В.1)—(В.11) и иных рекомендаций приложения В.

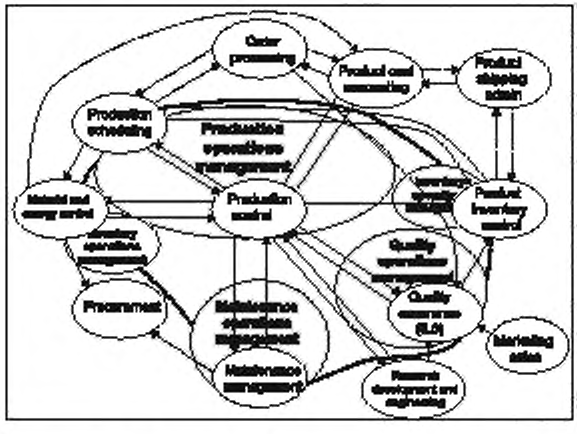
Г.6 Обработка и использование результатов прогнозирования

Результаты прогнозирования рисков должны быть удобны для обработки заказчиком системного анализа и/или аналитиком процесса управления решениями. Результаты представляют в виде гистограмм, графиков, таблиц и/или в ином виде, позволяющем анализировать зависимости рисков от изменения значений исходных данных при решении задач системного анализа. Результаты расчетов подлежат использованию для решения задач системного анализа — см. раздел 7, приложение Е и ГОСТ Р 59349.

Г.7 Примеры

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

Пусть некоторое предприятие организует управление производством, ориентируясь на требования ГОСТ Р МЭК 62264-1 по интеграции систем управления предприятием. Вербальное описание модели управления автоматизированным производством представлено на рисунке Г.1, полностью идентичном рисунку 8 из ГОСТ Р МЭК 62264-1—2014.



Order processing	Обработка заказов
Product cost accounting	Учет затрат на продукцию
Product shipping admin	Управление отгрузкой продукции
Production scheduling	Планирование производства
Production operations management	Управление производственными процессами
Material and energy control	Контроль материалов и энергии
Production control	Контроль производства
Inventory operations management	Управление товарно-материальными запасами
Product inventory control	Контроль товарных запасов
Quality operations management	Управление процессами контроля качества
Procurement	Материально-техническое снабжение
Maintenance operations management	Управление процессами технического обслуживания
Maintenance management	Управление техническим обслуживанием
Quality assurance (QA)	Обеспечение качества (QA)
Research development and engineering	Научно-исследовательские и опытно-конструкторские работы
Marketing sales	Маркетинг и продажи

Рисунок Г.1 — Вербальное описание управления автоматизированным производством по ГОСТ Р МЭК 62264-1

Не вдаваясь в детали интегрируемых систем управления в части производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации на предприятии, в рамках примера продемонстрированы отдельные подходы к системному анализу следующих действий рассматриваемого процесса управления решениями (см. 6.1.3):

- действие 1 — планирование управления решениями;
- действие 2 — сбор, обработка и анализ информации для принятия решений — прогнозирование рисков по ГОСТ Р 59341;
- действие 3 — принятие решений и управление решениями.

Проиллюстрированы возможности системного анализа в части прогнозирования:

- риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации;
- риска нарушения требований по защите информации;
- интегрального риска нарушения надежности реализации процесса управления решениями с учетом требований по защите информации.

При этом для оценки риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации в рамках примера выбраны следующие модели (см. рисунок Г.2):

- модели В.2.2—В.2.3 для анализа действий, связанных с планированием управления решениями (действие 1), принятием решений и управлением решениями (действие 3);
- модели, связанные со сбором, обработкой и анализом информации для принятия решений (действие 2) — по ГОСТ Р 59341.

Таким образом для проведения исследований из комплекса типовых действий процесса управления решениями искусственно выделены действия сбора, обработки и анализа информации. Их анализ добавлен с помощью алгоритма расчетов по методам В.2.4, В.2.5 (см. Г.7.2, Г.7.3).

Для прогнозирования риска нарушения требований по защите информации непосредственно используют модель и методы В.3 (см. Г.7.4), а для прогнозирования интегрального риска — метод В.4 (см. Г.7.5).

Такое формальное описание позволяет сформировать моделируемую систему в виде структуры следующих последовательных элементов, ассоциируемых с действиями процесса управления решениями по 6.1.3 (см. рисунок Г.3):

- для планирования процесса управления решениями:
  - 1-й элемент — действие 1 для производственного процесса;
  - 2-й элемент — действие 1 для процесса технического обслуживания;
  - 3-й элемент — действие 1 для процесса контроля качества;
  - 4-й элемент — действие 1 для процесса инвентаризации;
- для принятия решений и управления решениями:
  - 5-й элемент — действие 2 для производственного процесса;
  - 6-й элемент — действие 2 для процесса технического обслуживания;
  - 7-й элемент — действие 2 для процесса контроля качества;
  - 8-й элемент — действие 2 для процесса инвентаризации.

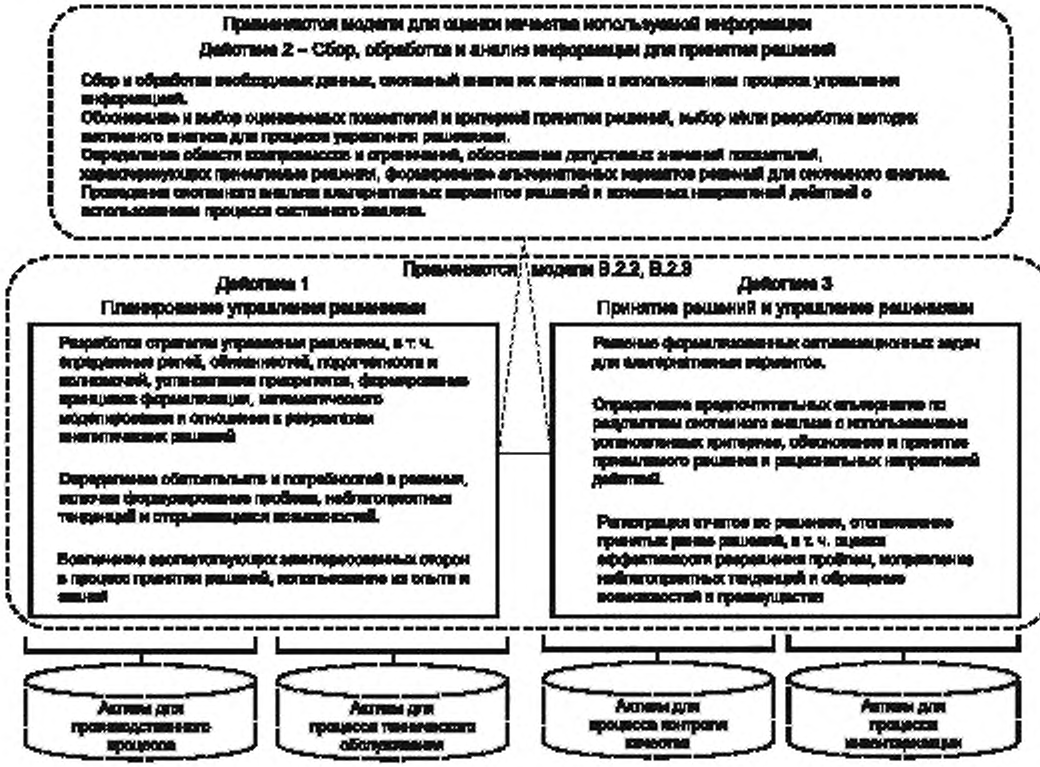


Рисунок Г.2 — Формальное описание комплекса действий для оценки риска нарушения надежности реализации процесса управления решениями



Рисунок Г.3 — Структура моделируемой системы без учета требований по защите информации

По определению надежность реализации процесса управления решениями моделируемой системы считается обеспеченной в течение заданного периода прогноза, если в течение этого периода «И» для производственного процесса, «И» для процесса технического обслуживания, «И» для процесса контроля качества, «И» для процесса инвентаризации обеспечена надежность реализации процесса, в том числе «И» по планированию управления решениями (по элементам 1, 2, 3, 4), «И» по принятию решений и управлению решениями (по элементам 5, 6, 7, 8). Причем надежность выполнения этих процессов при сохранении условий будет приемлемой в течение такого же периода и в будущем в жизненном цикле системы. Таким образом сам период прогноза для отдельного элемента может быть интерпретирован как относящийся и к стадиям создания этого элемента (по угрозам, свойственным этим стадиям), и к стадиям эксплуатации и выведения из эксплуатации (по потенциально возможным угрозам). При моделировании подтверждается приемлемость решений, сохранение возможностей и обеспечение гарантий удержания риска в допустимых пределах.

С учетом соизмеримости возможных ущербов цели прогнозирования рисков сформулированы руководством предприятия следующим образом. В условиях существующей неопределенности:

- количественно оценить риски нарушения надежности реализации процесса управления решениями на предприятии без учета качества используемой информации по результатам сбора, обработки и анализа инфор-

мации для принятия решений и учета требований по защите информации (как поэлементно, так и в целом для процесса);

- количественно оценить риски нарушения надежности реализации процесса управления решениями на предприятии с учетом качества используемой информации по результатам сбора, обработки и анализа информации для принятия решений (в целом для процесса, но без учета требований по защите информации);
- количественно оценить риски нарушения требований по защите информации (как поэлементно, так и в целом для процесса управления решениями);
- количественно оценить риски нарушения надежности реализации процесса управления решениями на предприятии с учетом требований по защите информации (в целом для процесса);
- определить такой период, при котором обеспечиваются гарантии удержания риска в допустимых пределах;
- определить критичные условия в развитии различных угроз.

Тем самым выполнены шаги 1, 2 настоящих методических указаний.

Пример 1 иллюстрирует прогнозирование риска нарушения надежности реализации процесса управления решениями без учета качества используемой информации и требований по защите информации. Пример 2 показывает, как при прогнозировании риска нарушения надежности реализации процесса управления решениями можно дополнительно учесть качество используемой информации по результатам сбора, обработки и анализа информации для принятия решений. В примере 3 продемонстрировано прогнозирование риска нарушения требований по защите информации. Пример 4 иллюстрирует прогнозирование интегрального риска нарушения реализации процесса управления решениями с учетом требований по защите информации.

Г.7.2 Пример 1. Прогнозирование риска нарушения надежности реализации процесса управления решениями без учета качества используемой информации и требований по защите информации проиллюстрировано для структуры моделируемой системы, представленной на рисунке Г.3. Выполняя шаг 3 настоящих методических указаний, выявлены возможные угрозы, критично влияющие на безопасность каждого из структурных элементов. При этом учтены угрозы, связанные не только с причинами программно-технических, технологических и человеческих ошибок, но и гипотетичные угрозы, связанные с последствиями этих ошибок. Исходные данные по каждому из 8 составных элементов представлены в таблице Г.1. В ней учтены исходные данные примеров из стандарта ГОСТ Р 59347—2021 (приложение Г), связанные с характеристиками типовой архитектуры предприятия согласно ГОСТ Р ИСО 15704.

Таблица Г.1 — Исходные данные для прогнозирования риска нарушения надежности реализации процесса управления решениями без учета качества используемой информации и требований по защите информации

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
σ — частота возникновения источников угроз нарушения надежности реализации процесса	5 раз в год (из-за недостаточной квалификации, компетенции или знаний для планирования управления решениями или из-за проблем со здоровьем лиц, планирующих решения в производственном процессе) / 1 раз в год (из-за проблем со здоровьем лиц, планирующих решения в процессе технического обслуживания) / 1 раз в год (из-за проблем со здоровьем лиц, планирующих решения в процессе контроля качества) / 1 раз в год (из-за проблем со здоровьем лиц, планирующих решения в процессе инвентаризации) - это угрозы программно-технических, технологических и человеческих ошибок на уровне планирования решений	2 раза в год (из-за недостаточной квалификации, компетенции или знаний для решения задач или из-за проблем со здоровьем лиц, принимающих решения в производственном процессе) / 1 раз в год (из-за проблем со здоровьем лиц, принимающих решения в процессе технического обслуживания) / 1 раз в год (из-за проблем со здоровьем лиц, принимающих решения в процессе контроля качества) / 1 раз в год (из-за проблем со здоровьем лиц, принимающих решения в процессе инвентаризации) - это угрозы ущерба от принятия необоснованных решений

Продолжение таблицы Г.1

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
β — среднее время развития угроз для элемента с момента возникновения источников угроз до нарушения с возможным ущербом	2 нед (что соизмеримо со временем математического моделирования или макетных экспериментов, обосновывающих планы) / 1 год (что соизмеримо со временем между критичными ошибками в планировании технического обслуживания) / 1 год (что соизмеримо со временем между критичными ошибками в планировании контроля качества) / 1 год (что соизмеримо со временем между критичными ошибками в планировании инвентаризации) - это среднее время до возможного ущерба после критичных программно-технических, технологических или человеческих ошибок, допущенных при планировании	6 мес (что соизмеримо со временем постепенного отказа производственного оборудования с учетом возможных проблем в техническом обслуживании) / 6 мес (что объясняется сохранением минимальных возможностей системы функционировать в устаревшей среде без обновлений, осуществляемых при техническом обслуживании) / 2 мес (что объясняется средним временем до возможных рекламаций из-за критичных ошибок при контроле качества) / 6 мес (что объясняется средним временем до производственных простоев из-за критичных ошибок при инвентаризации) - это среднее время до возможного ущерба после критичных программно-технических, технологических или человеческих ошибок, допущенных при принятии решений
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей элемента	8 ч / 8 ч / 8 ч / 8 ч - это время определяется регламентом контроля готовности персонала к работе — 1 раз за смену при 8-часовом рабочем дне	1 ч — определяется регламентом контроля процесса функционирования оборудования / 1 нед — определяется регламентом технического обслуживания / 1 нед — определяется регламентом отчетности службы контроля качества на предприятии / 1 нед — определяется регламентом отчетности службы контроля инвентарного учета на предприятии
$T_{диаг}$ — среднее время диагностики состояния элемента	10 мин / 10 мин / 10 мин / 10 мин - определяется временем медицинского обследования перед работой	30 с — означает длительность автоматического контроля целостности оборудования в производственном процессе / 1 ч — диагностика состояния оборудования при техническом обслуживании / 30 с — означает длительность автоматического контроля целостности оборудования / 30 с — означает длительность автоматической инвентаризации активов

Окончание таблицы Г.1

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
$T_{восст}$ — среднее время восстановления элемента после выявления нарушений	30 мин / 30 мин / 30 мин / 30 мин - это время замены человека, отстраненного от выполнения обязанностей, и возложения необходимых функциональных обязанностей на заменяющего человека для выполнения функций планирования	4 ч — среднее время восстановления оборудования после сбоя или отказа / 8 ч — это время восстановления нарушенного процесса технического обслуживания / 30 мин — это время переинсталляции программного обеспечения системы контроля качества / 8 ч — это время восстановления нарушенного процесса инвентаризации
$T_{зад}$ — задаваемая длительность периода прогноза	от 1 месяца до 1 года (для определения периода, при котором сохраняются гарантии удержания риска нарушения надежности реализации процесса в допустимых пределах)	

Выполняя шаг 4 настоящих методических указаний, прогнозирование риска нарушения надежности реализации процесса управления решениями (без учета качества используемой информации и требований по защите информации) выполнено с использованием расчетных соотношений (В.1)—(В.9) согласно рекомендациям В.2.2, В.2.3 и В.2.4.

Анализ результатов расчетов показал, что для производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации на предприятии по ГОСТ Р МЭК 62264-1 в вероятностном выражении риск нарушения надежности реализации рассматриваемых действий процесса управления решениями в течение года составит около 0,142 (см. рисунок Г.4), составляя для 1-го элемента — 0,058, а для 7-го элемента 0,053, что совместно составляет более 77 % от общего риска по всем элементам. Это означает, что действия по планированию управления решениями в производственном процессе (элемент 1) и действия по принятию решений и управлению решениями в процессе контроля качества (элемент 7) являются определяющими в общем риске нарушения надежности реализации рассматриваемого процесса управления решениями. С учетом специфики производства именно в элементах 1 и 7 содержатся искомые критичные условия в развитии различных угроз для предприятия (см. условия в таблице Г.1). По элементам 2—6, 8 значения оцениваемого риска не превышают 0,019. При изменении периода прогноза от 1 мес до года риск за все действия возрастает от 0,012 до 0,142. Для допустимого риска на уровне 0.05 обоснован период до 117 дней, при котором обеспечиваются гарантии удержания риска в допустимых пределах для условий таблицы Г.1.

Примечание — Пилообразный характер зависимости риска от периода прогноза на рисунке Г.5 объясняется учетом периодического контроля и восстановления целостности моделируемой системы при диагностике и тем, что в модели В.2.3 при расчетах используется целое количество диагностик, входящих в период прогноза. Сразу после диагностики риск снижается, со временем до следующей диагностики — возрастает. Именно это является причиной пилообразности.

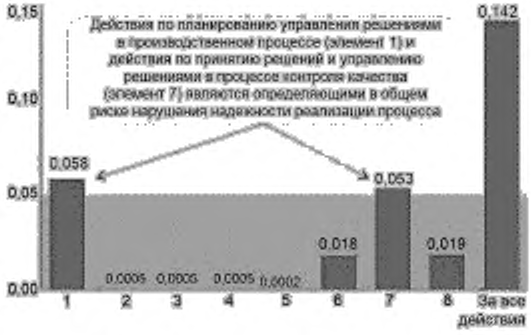


Рисунок Г.4 — Оценки риска без учета качества используемой информации и требований по защите информации (период прогноза 1 год)

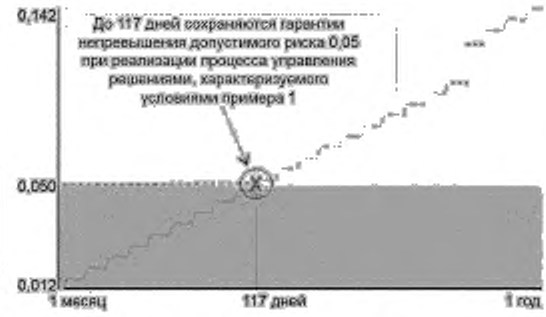


Рисунок Г.5 — Зависимость риска от периода прогноза длительностью от 1 месяца до 1 года

Г.7.3 Пример 2 показывает последовательность возможных действий системного анализа, направленных на определение того, как дополнительно к результатам примера 1 можно учесть качество используемой информации (получаемой по результатам сбора, обработки и анализа информации для принятия решений).

По факту в рамках рассматриваемого процесса управления решениями используется другой процесс — процесс управления информацией (при сборе, обработке и анализе информации для принятия решений). Для учета этого вложенного процесса управления информацией используют модели и методы стандарта ГОСТ Р 59341. В результате их применения вычисляют:

- коэффициенты надежности $Z_{\text{над. предст}}(T_{\text{зад}})$ и своевременности $Z_{\text{своевр}}$ представления информации (по моделям и методам ГОСТ Р 59341—2021, В.3.2 и В.3.3 приложения В);

- вероятности того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{\text{полн}}$ (по ГОСТ Р 59341—2021, В.3.4 приложения В);

- вероятности сохранения актуальности информации в системе на момент ее использования $P_{\text{акт}}$ (по ГОСТ Р 59341—2021, В.3.5 приложения В);

- вероятности отсутствия ошибок в информации после ее контроля $P_{\text{безош}}$ (по ГОСТ Р 59341—2021, В.3.6 приложения В);

- вероятности получения корректных результатов обработки информации $P_{\text{корр}}$ (по ГОСТ Р 59341—2021, В.3.7 приложения В);

- вероятности безошибочных действий ответственных лиц в течение заданного периода прогноза $P_{\text{чел}}(T_{\text{зад}})$ (по ГОСТ Р 59341—2021, В.3.8 приложения В).

Риск нарушения надежности реализации процесса управления решениями с учетом качества используемой информации, но без учета требований по защите информации определяют по формуле (В.10) — см. В.2.5.

Для применения формулы (В.10) в рамках примера 2 значение вероятности нарушения надежности реализации процесса управления решениями в течение периода прогноза без учета качества используемой информации и требований по защите информации $R_{\text{надежн В.2.2-В.2.3}}(T_{\text{зад}})$ использован результат примера 1, где $R_{\text{надежн В.2.2-В.2.3}}(T_{\text{зад}})$ составляет 0,012 для периода прогноза $T_{\text{зад}}$, равного одному месяцу. Недостающее для применения формулы (В.10) значение вероятности нарушения надежности реализации процесса управления информацией в течение периода прогноза без учета требований по защите информации $R_{\text{наруш УИ}}(T_{\text{зад}})$ в общем случае вычисляют по моделям и рекомендациям ГОСТ Р 59341—2021 В.3.2—В.3.8, В.3.10 приложения В. Чтобы не приводить излишние детали оценки надежности и своевременности представления полной и достоверной информации для принятия решений, в примере 2 использованы результаты из ГОСТ Р 59341—2021 (см. примеры Г.7.2—Г.7.8 приложения Г), в которых в качестве аналога моделируемой системы проанализирована система дистанционного контроля. А именно — для примера 2 были приняты следующие результаты:

- коэффициенты надежности $Z_{\text{над. предст}}(T_{\text{зад}} = 1$ месяц) и своевременности $Z_{\text{своевр}}$ представления информации равны единице (с учетом задаваемого допустимого уровня надежности и своевременности представления информации);

- вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений, $P_{\text{полн}} = 0{,}95$;

- вероятность сохранения актуальности информации в системе на момент ее использования $P_{\text{акт}} = 0{,}95$;

- вероятность отсутствия ошибок в информации после ее контроля $P_{\text{безош}} = 0{,}96$;

- вероятность получения корректных результатов обработки информации $P_{\text{корр}} = 0{,}96$;

- вероятность безошибочных действий ответственных лиц в течение заданного периода прогноза $P_{чел}$ ($T_{зад}$ = 1 месяц) = 0,96.

В предположении отсутствия задаваемых допустимых требований к полноте и достоверности используемой информации и безошибочности действий ответственных лиц в рамках рассматриваемого процесса управления решениями вероятность нарушения надежности реализации процесса управления информацией в течение периода прогноза, равного 1 месяцу, без учета требований по защите информации

$$R_{наруш\ УИ}(T_{зад} = 1\ месяц) = 1 - P_{над.\ предст}(T_{зад}) \cdot C_{своевр} \cdot P_{полн} \cdot P_{акт} \cdot P_{безош} \cdot P_{корр} \cdot P_{чел}(T_{зад}) =$$
$$= 1 - 1 \cdot 1 \cdot 0{,}95 \cdot 0{,}95 \cdot 0{,}96 \cdot 0{,}96 \cdot 0{,}96 \approx 1 - 0{,}7985 \approx 0{,}2015.$$

Подставляя значения 0,012 и 0,2015 в формулу (В.10), в примере 2, получено

$$R_{надежн}(T_{зад}) = 1 - (1 - 0{,}012) \cdot (1 - 0{,}2015) \approx 0{,}211.$$

В итоге по результатам системного анализа примеров 1 и 2 вероятность нарушения надежности реализации процесса управления решениями $R_{надежн}(T_{зад})$ в течение периода прогноза, равного 1 месяцу, без учета требований по защите информации составляет около 0,211. При этом более 95 % от этого значения составляет риск, определяемый достигаемым уровнем качества используемой информации. Это означает, что в случае неудовлетворенности достигаемой надежностью реализации рассматриваемого процесса управления решениями первоочередные усилия системной инженерии следует направить именно на повышение качества используемой информации. При этом заданию подлежат требования к допустимому уровню полноты и достоверности используемой информации и уровню безошибочности действий ответственных лиц, связанных со сбором и обработкой информации. Если же это качество используемой информации признается приемлемым или неулучшаемым (например, по причинам технологической невозможности или по экономическим соображениям), то с достигаемым качеством соглашаются и риски нарушения этого качества не учитывают (т. е. ими пренебрегают) при дальнейшем системном анализе. В этом случае $R_{надежн}(T_{зад})$ = 0,012.

Г.7.4 Пример 3. Продолжая примеры 1 и 2, прогнозирование риска нарушения требований по защите информации проиллюстрировано для комплекса действий по планированию процесса управления решениями, принятию решений и непосредственно управлению решениями по ГОСТ Р МЭК 62264-1. При этом осуществлена привязка к структуре действий и защищаемых активов, определенных на рисунках Г.2, Г.6. Расчеты выполнены с применением рекомендаций В.3.

Примечание — Наряду с моделями, рекомендуемыми в В.3, по решению аналитика могут быть использованы модели, рекомендуемые ГОСТ Р 59341, ГОСТ Р 59346 или иные модели, учитывающие специфику создаваемой (модернизируемой) и/или применяемой системы и/или системы, выводимой из эксплуатации.

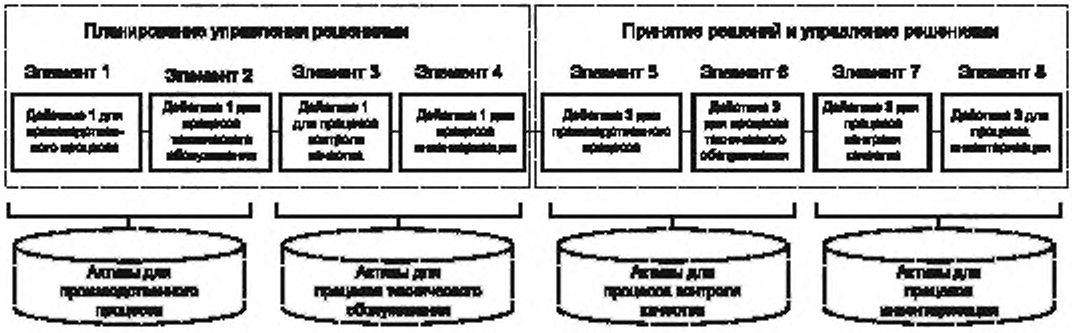


Рисунок Г.6 — Структура моделируемой системы

Исходные данные по каждому из восьми составных элементов моделируемой системы, учитывающие возможные уязвимости в технологиях защиты активов и сопровождаемые поясняющими комментариями, представлены в таблице Г.2.

Таблица Г.2 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе управления решениями

Исходные данные	Значения и комментарии	
	для 1-го/ 2-го/ 3-го/ 4-го элементов при планировании управления решениями	для 5-го/ 6-го/ 7-го/ 8-го элементов при принятии решений и управлении решениями
σ — частота возникновения источников угроз нарушения требований по защите информации	1 раз в год (что соизмеримо с частотой технического отказа производственного оборудования) / 1 раз в год (что соизмеримо с частотой ошибок со стороны специалиста-планировщика средней квалификации) / 2 раза в год (что соизмеримо с частотой ошибок со стороны контролера средней квалификации) / 2 раза в год (что соизмеримо с частотой ошибок по планированию в части инвентаризации со стороны специалиста средней квалификации) - это угрозы ущерба в результате нарушения требований по защите информации при планировании управления решениями с использованием активов	1 раз в год (что соизмеримо с частотой технического отказа производственного оборудования) / 1 раз в 5 лет (что объясняется маскировкой под отказы в процессе технического обслуживания системы специалистами высокой квалификации) /1 раз в год (что соизмеримо с частотой ошибок со стороны контролера высокой квалификации) / 1 раз в год (что соизмеримо с частотой ошибок по инвентаризации со стороны специалиста высокой квалификации) - это угрозы ущерба в результате нарушения требований по защите информации при принятии решений и управлении решениями с использованием активов
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	1 сут / 1 сут / 1 сут / 1 сут (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток) - это время до ущерба после возникновения признаков угроз при планировании управления решениями с использованием активов	1 сут / 1 сут / 1 сут / 1 сут (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее суток) - это время до ущерба после возникновения признаков угроз при принятии решений и управлении решениями с использованием активов
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	1 ч / 1 ч / 1 ч / 1 ч - определяется регламентом контроля целостности программного обеспечения и активов, используемых при планировании управления решениями	1 ч / 1 ч / 1 ч / 1 ч - определяется регламентом контроля целостности программного обеспечения и активов, используемых при принятии решений и управлении решениями
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы защиты информации	30 с / 30 с / 30 с / 30 с - автоматический контроль целостности программного обеспечения и активов, используемых при планировании управления решениями	30 с / 30 с / 30 с / 30 с - автоматический контроль целостности программного обеспечения и активов, используемых при принятии решений и управлении решениями
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	5 мин / 5 мин / 5 мин / 5 мин (включая перезагрузку программного обеспечения и восстановление данных)	5 мин / 5 мин / 5 мин / 5 мин (включая перезагрузку программного обеспечения и восстановление данных)
$T_{зад}$ — задаваемая длительность периода прогноза	от одного до четырех месяцев (для определения периода, при котором сохраняются гарантии удержания риска в допустимых пределах для обеспечения нормы эффективности защиты информации)	

Прогнозирование риска нарушения требований по защите информации в рассматриваемом процессе управления решениями выполнено с использованием рекомендаций В.3.

Анализ результатов расчетов показал, что для производственного процесса, процесса технического обслуживания, процесса контроля качества и процесса инвентаризации в вероятностном выражении риск нарушения требований по защите информации в течение месяца составит около 0,016 (см. рисунок Г.7), составляя для элементов 1—5, 7—8 — около 0,002, для 6-го элемента — 0,0003, т. е. все активы защищены в сравнительно равнопрочной степени. При увеличении периода прогноза от одного до четырех месяцев риск возрастает от 0,016 до 0,062. Для допустимого риска на уровне 0,05 обоснован период до 96 дней, при котором сохраняются гарантии удержания рисков в допустимых пределах для условий примера 3 (см. рисунок Г.8).

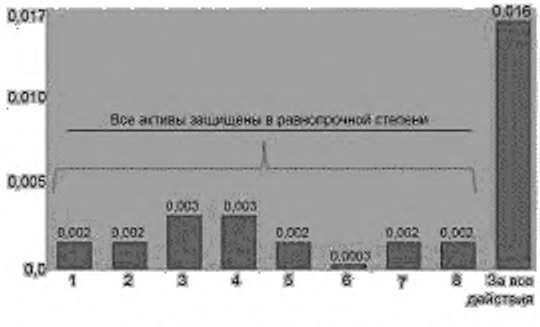


Рисунок Г.7 — Оценки риска нарушения требований по защите информации в течение месяца

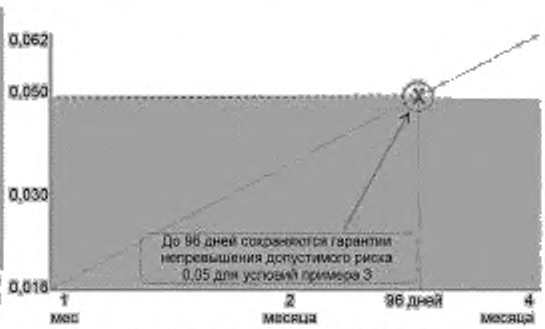


Рисунок Г.8 — Зависимость риска от периода прогноза длительностью от 1 до 4-х месяцев

Г.7.5 Пример 4. В продолжение примеров 1, 2 и 3 интегральный риск $R_{интегр}(T_{зад})$ нарушения реализации процесса управления решениями с учетом требований по защите информации рассчитан с использованием рекомендаций В.4.

Учитывая, что периода прогноза $T_{зад}$ = 1 месяц, по результатам 1-го и 2-го примеров выбирается значение $R_{надежн}(T_{зад})$ = 0,211, а по результатам 3-го примера $R_{наруш}(T_{зад})$ = 0,016, то по формуле (В.10)

$$R_{интегр}(T_{зад}) = 1 - (1 - 0{,}211) \cdot (1 - 0{,}016) \approx 0{,}224.$$

В итоге интегральный риск нарушения надежности реализации процесса управления решениями в течение одного месяца с учетом требований по защите информации составит в вероятностном выражении около 0,224. При этом риск нарушения требований по защите информации (0,016) в 13 раз меньше риска нарушения надежности реализации процесса управления решениями без учета требований по защите информации (0,211). Основной причиной высокого интегрального риска, который существенно превышает риски нарушения надежности производственного оборудования, является сравнительно невысокий уровень качества используемой информации (см. анализ этого качества в примере 3). Если этот уровень качества признается приемлемым или неулучшаемым и заказчиком (или аналитиком) принимается решение не учитывать приемлемое достижимое качество используемой информации в интегральных расчетах, то тогда возможно применение другой полученной в примере 2 оценки, а именно: $R_{надежн}(T_{зад})$ = 0,012. И тогда

$$R_{интегр}(T_{зад}) = 1 - (1 - 0{,}012) \cdot (1 - 0{,}016) \approx 0{,}028.$$

Это меньше установленного допустимого уровня 0,05, причем при аналогичных ущербах и обоснованных затратах надежность реализации процесса управления решениями оказывается соизмеримой в вероятностном выражении с эффективностью защиты информации. Это подтверждает сбалансированность планируемых к применению или применяемых технических решений с точки зрения достижения целей системной инженерии.

Таким образом, с помощью приведенных четырех примеров продемонстрированы отдельные аналитические возможности методов и моделей, применение которых упорядочено в настоящих методических указаниях.

Примечание — Другие примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Г.8 Материально-техническое обеспечение

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

- результаты обследования, концепция создания, технический облик и/или ТЗ на разработку для создаваемой системы, конструкторская и эксплуатационная документация для существующей системы (используют для формирования исходных данных при моделировании);

- модель угроз безопасности информации (используют для формирования необходимых исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);

- записи из системного журнала учета предпосылок, инцидентов и аварий при функционировании системы, связанных с нарушением требований по защите информации (используют для формирования исходных данных при моделировании);

- планы ликвидации нарушений, инцидентов и аварий, связанных с нарушением требований по защите информации, и восстановления целостности системы (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);

- обязанности должностных лиц и инструкции по защите информации при выполнении процесса (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);

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

Г.9 Отчетность

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

Приложение Д
(справочное)

Типовые допустимые значения показателей рисков для процесса управления решениями

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

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

Требования системной инженерии при допустимых рисках, свойственных конкретной системе или ее аналогу и 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 иным соображениям) или невозможной ориентация на допустимые риски, свойственные системе-эталону. Вследствие этого минимальной гарантией обеспечения качества и безопасности реализации процесса управления решениями является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Типовые допустимые значения количественных показателей рисков для процесса управления решениями отражены в таблице Д.1. При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые. В этом случае для задаваемых при моделировании условий имеет место гарантия качества и безопасности реализации рассматриваемого процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Пример задания допустимых значений рисков

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

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса управления решениями

Е.1 Методика прогнозирования риска нарушения требований по защите информации в процессе управления решениями.

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

Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса управления решениями с учетом требований по защите информации).

Е.4 Методики выявления явных и скрытых недостатков процесса управления решениями с использованием прогнозирования рисков.

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

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

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[16] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»

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

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

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

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

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

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

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

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

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

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

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

Ключевые слова: актив, безопасность, защита информации, модель, риск, система, системная инженерия, процесс управления решениями

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

Сдано в набор 29.04.2021. Подписано в печать 13.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru