ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59347— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ

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 30 апреля 2021 г. № 333-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 определения архитектуры системы 7
5 Общие требования системной инженерии по защите информации в процессе определения архитектуры системы 9
6 Специальные требования к количественным показателям 10
7 Требования к системному анализу 12
Приложение А (справочное) Пример перечня защищаемых активов 14
Приложение Б (справочное) Пример перечня угроз 15
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 16
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса определения архитектуры системы 24
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса определения архитектуры системы 34
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса определения архитектуры системы 35
Библиография 36

Введение

Настоящий стандарт расширяет комплекс национальных стандартов системной инженерии по защите информации при планировании и реализации процессов в жизненном цикле различных систем. Выбор и применение реализуемых процессов для системы в ее жизненном цикле осуществляют по ГОСТ Р 57193. Методы системной инженерии в интересах защиты информации применяют:

- для процессов соглашения — процессов приобретения и поставки продукции и услуг для системы — по ГОСТ Р 59329;

- для процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, управления инфраструктурой, управления портфелем, управления человеческими ресурсами, управления качеством, управления знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;

- для процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343;

- для технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения 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 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. Для процесса определения архитектуры системы — по настоящему стандарту.

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

Для планируемого и реализуемого процесса определения архитектуры применение настоящего стандарта при создании (модернизации, развитии) и эксплуатации системы обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ

System engineering. Protection of information in system architecture definition process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные методические положения системного анализа для процесса определения архитектуры 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) и эксплуатации систем и реализующими процесс определения архитектуры системы, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем (см. примеры систем в [1]—[26]).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

Издание официальное

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

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

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

ГОСТ Р ИСО 14813-1 Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспортных систем. Часть 1. Сервисные домены в области интеллектуальных транспортных систем, сервисные группы и сервисы

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 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 56875 Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий

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

ГОСТ Р 57100/ISO/IEC/IEEE 42010:2011—2016 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 59338 Системная инженерия. Защита информации в процессе управления решениями

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

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

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

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

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

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

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

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

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 34.003, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 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

архитектура (системы): Основные понятия или свойства системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития.

[ГОСТ Р 57100—2016/ISO/IEC/IEEE 42010:2011, пункт 3.5]

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.3

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

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

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

[ГОСТ Р 57193—2016, пункт 4.1.42]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.5

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.6

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.7

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

3.1.9 **моделируемая система:** Система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения.

Примечание — В качестве модели системы могут выступать формализованные сущности, объединенные целевым назначением. Например, при проведении системного анализа в принимаемых допущениях, ограничениях и предположениях модель может формально описывать взаимодействующие подсистемы, процесс, функциональные действия процесса, множество активов и/или выходных результатов процесса или множество этих, или иных сущностей в их целенаправленном применении в задаваемых условиях.

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

3.1.11

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.12

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.13

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

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

[ГОСТ Р 57193—2016, пункт 4.1.50]

3.1.14

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.15 **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.

3.1.16

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]

3.1.17

структура архитектуры: Условности, принципы и практики для описания архитектур, установленные в пределах заданной области применения и/или объединения заинтересованных сторон.

Примеры

1 Обобщенная стандартная архитектура предприятия и методологии (GERAM) [ИСО 15704] является некоторой структурой архитектуры.

2 Эталонная модель открытой распределенной обработки (RM—ODP) [ИСО/МЭК 10746] является некоторой структурой архитектуры.

[ГОСТ Р 57100—2016, пункт 3.4]

3.1.18

точка зрения на архитектуру: Рабочий продукт, устанавливающий условности конструирования, интерпретации и использования архитектурного представления для структуризации определенных системных интересов.

[ГОСТ Р 57100—2016, пункт 3.6]

3.1.19

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]

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

3.1.21

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 определения архитектуры системы

4.1 Общие положения

Организации используют процесс определения архитектуры в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения ее безопасности, качества и эффективности. В процессе определения архитектуры системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

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

Формирование выходных результатов процесса определения архитектуры 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. Количественную оценку интегрального риска с учетом требований по защите информации в процессе определения архитектуры системы осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355 с учетом специфики системы (см., например, [21]—[26]).

4.2 Цели процесса и назначение мер защиты информации

4.2.1 Формулирование целей процесса определения архитектуры системы осуществляют с использованием 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 и с учетом специфики системы.

В общем случае целями процесса определения архитектуры являются подготовка возможных вариантов архитектуры системы, выбор из этих вариантов приемлемого варианта (одного или нескольких, если это необходимо), который структурирует интересы заинтересованных сторон, отвечает системным требованиям и выражает во множестве согласованных представлений различные точки зрения на систему. Определение архитектуры может быть применено на различных уровнях абстракции, акцентируя внимание на деталях, необходимых для принятия решений на этом уровне.

4.2.2 Меры защиты информации в процессе определения архитектуры системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, 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.

4.3 Стадии и этапы жизненного цикла системы

Процесс определения архитектуры системы может быть использован на стадиях разработки концепции (концептуальных положений) и разработки (в рамках эскизного и/или технического проектирования), а также на стадии эксплуатации для анализа, совершенствования и развития архитектурных решений. Этапы работ по созданию (модернизации, развитию) и эксплуатации системы 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 определения архитектуры может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.4 Основные принципы

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

4.5 Основные усилия для обеспечения защиты информации

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

- на определении выходных результатов и действий, предназначенных для достижения целей процесса и защиты активов, информация которых или о которых необходима для достижения этих целей;
- выявлении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для активов, подлежащих защите, выходных результатов и выполняемых действий процесса;

- определении и прогнозировании рисков, подлежащих системному анализу;
- проведении системного анализа для обоснования мер, направленных на противодействие угрозам и достижение целей процесса.

5 Общие требования системной инженерии по защите информации в процессе определения архитектуры системы

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 по защите информации 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 определения архитектуры системы 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 определения архитектуры в системах искусственного интеллекта необходимо гарантированно подтверждать достаточность автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации и пр.), учитывать возможность повышения уровня конфиденциальности данных в процессе их обработки в системе искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации), 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 определения архитектуры системы и поддержке при этом эффективности защиты информации.

Требования системной инженерии по защите информации в процессе определения архитектуры системы включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе определения архитектуры системы формируют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 14258, ГОСТ Р ИСО 14813-1, ГОСТ Р 15.301, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56875, 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 определения архитектуры системы.

Примечание — В состав активов могут быть включены активы, используемые для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика, например привлекаемые информационные системы и/или базы данных 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 34.201, 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 требований 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, ГОСТ Р МЭК 62264-1, [20]—[24].

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

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

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, 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 ИСО 31000, 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.

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 определения архитектуры определен в 6.3.

Типовые модели и методы системного анализа процесса определения архитектуры системы, методические указания по прогнозированию рисков, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д, Е. Характеристики мер и действий по защите информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по реализуемым процессам, исходя из возможных условий их реализации.

6 Специальные требования к количественным показателям

6.1 Общие положения

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

6.1.2 В общем случае основными выходными результатами процесса определения архитектуры системы являются.

- описания для вариантов архитектуры, в соответствии с которыми выполняют идентификацию элементов системы, определяют контекст, границы и внешние взаимодействия системы (по ГОСТ Р 57100);
- общее описание системы, функциональная структура, постановки задач;
- точки зрения на архитектуру, архитектурные представления и модели системы;
- описание автоматизируемых функций, организационная структура (по ГОСТ 34.201);
- схема деления системы, описание системных элементов и порядка их взаимодействия между собой и с внешним окружением;
- спецификации внутренних и внешних интерфейсов для каждого системного элемента;
- чертежи общего вида, схемы (по ГОСТ 2.102);
- системные требования, понятия, свойства, характеристики, функции и/или ограничения, распределенные по элементам системы, описание системы защиты информации в процессе определения системных требований (по ГОСТ Р 59346);
- результаты верификации между системными требованиями и архитектурой системы;
- материалы в эскизный и/или технический проекты системы и/или действующий макет, модели и/или прототипы архитектуры системы;

- отчеты по анализу системных требований;
- требования к обеспечивающим системам или системным элементам, необходимым для выполнения действий процесса;
- карта прослеживаемости элементов архитектуры с требованиями заинтересованных сторон и системными требованиями;
- отчет по архитектуре системы с соответствующими обоснованиями.

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

- подготовительные действия, включая:
- анализ необходимой информации (исследования рынка, промышленных проектов, планов и намерений конкурентов, научных результатов, организационной политики и директив, нормативных и юридических ограничений, функциональной концепции и эксплуатационной среды системы),
- уточнение требований заинтересованных сторон, связанных с архитектурой, таких как требования к функционированию (например, надежности, безопасности, эффективности), сопровождению, развитию системы и окружающей среды, производству,
- выработку подходов к разработке и стратегии модернизации и развития архитектуры системы,
- определение критериев оценки вариантов архитектуры, основанных на учете интересов заинтересованных сторон и основных системных требований,
- определение требований и взаимодействий для обеспечивающих систем и/или услуг, использование которых предполагается для поддержки процесса определения архитектуры. Получение или приобретение доступа к обеспечивающим системам и/или услугам;
- разработку описаний для вариантов архитектуры и/или разработку действующих моделей (и/или прототипов) архитектуры системы, включая:
- выбор, приспосабливание или разработку точек зрения на архитектуру и необходимых моделей,
- определение потенциальной структуры архитектуры, которая будет использоваться в разрабатываемых моделях и архитектурных представлениях,
- выбор или разработку методик и инструментариев для поддержания моделирования,
- выбор, приспосабливание или разработку моделей и представлений для архитектурных вариантов,
- согласование моделей архитектуры и архитектурных представлений друг с другом;
- оценку вариантов архитектуры системы, включая:
- оценку каждого варианта архитектуры применительно к установленным ограничениям и требованиям, а также к интересам заинтересованных сторон с использованием установленных критериев оценки,
- выбор и обоснование предпочтительного варианта архитектуры и основных архитектурных решений;
- управление выбранной архитектурой системы, включая:
- официальное согласование архитектуры с заинтересованными сторонами;
- поддержание соответствия и полноты архитектурных сущностей и их архитектурных характеристик.

Примечание — Сущности, которые подлежат проверке могут быть не только техническими, но также юридическими, экономическими, организационными и эксплуатационными, являющимися обычно частью интересов и требований заинтересованных сторон;

- поддержание стратегии определения и оценки архитектуры системы.

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).

6.2 Требования к составу показателей

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

Эффективность защиты информации оценивают с помощью количественных показателей, которые позволяют сформировать представление о текущих и потенциальных проблемах или о возможных причинах недопустимого снижения эффективности на ранних этапах проявления явных и скрытых угроз

безопасности информации, когда можно предпринять предупреждающие корректирующие действия. Дополнительно могут быть использованы вспомогательные статистические данные, характеризующие события, которые уже 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 определения архитектуры системы без учета требований по защите информации;
- риск нарушения требований по защите информации в процессе определения архитектуры системы;
- интегральный риск нарушения реализации процесса определения архитектуры системы с учетом требований по защите информации.

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

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

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

6.4 Требования к источникам данных

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

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

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к системному анализу

Требования к системному анализу процесса определения архитектуры системы включают:

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

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

При обосновании и формулировании конкретных требований к системному анализу дополнительно руководствуются рекомендациями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 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 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе определения архитектуры 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) архитектуры системы;
- финансовые и плановые документы, связанные с проведением работ по созданию (модернизации, развитию) архитектуры системы;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем — по ГОСТ 34.601);
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101 с учетом специфики 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;
- 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 определения архитектуры системы может включать (в части, свойственной этому процессу):

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275;

- угрозы государственным информационным системам, информационным системам персональных данных, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимым объектам критической информационной инфраструктуры Российской Федерации — по [21]—[24];

- угрозы безопасности функционирования программного обеспечения, оборудования и коммуникаций, используемых в процессе разработки и эксплуатации системы, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124;

- угрозы безопасности информации при подготовке и обработке документов — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124;

- 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 конкретной приобретающей стороне (заказчику), информация и информационные системы которого были скомпрометированы;

- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги;

- угрозы, связанные с нарушением интеллектуальной собственности;

- прочие соответствующие угрозы безопасности информации и уязвимости для информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов из банка данных угроз, сопровождаемого государственным регулятором.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Основные положения

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

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

В.1.2 Для расчета этих показателей рисков исследуемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. Модели и методы системного анализа таких систем используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики по процессам и возможным условиям их реализации.

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

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

В.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, включая требования по защите информации);
- в условиях неопределенностей возникновение и разрастание различных угроз описывается в терминах случайных событий;
- для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и/или защитных преград, предназначенных для воспрепятствования реализации угроз.

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

В.1.5 В подразделах В.2.2, В.2.3 приведены математические модели для прогнозирования рисков в системе, представляемой в виде «черного ящика». Модель В.2.2 для прогнозирования рисков при отсутствии какого-либо контроля является частным случаем модели в В.2.3 при реализации технологии периодического системного контроля. Модель подраздела 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 определения архитектуры системы без учета требований по защите информации, в В.3 приведены способы прогнозирования риска нарушения требований по защите информации в процессе (в т. ч. с использованием моделей В.2). Методы прогнозирования интегрального риска нарушения реализации процесса определения архитектуры системы с учетом требований по защите информации представлены в В.4. При этом интегральный риск нарушения реализации процесса определения архитектуры системы с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса определения архитектуры системы 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 определения архитектуры системы.

В.1.9 Другие возможные подходы и подходы, подобные изложенным в В.2, В.3 для оценки рисков описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 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 определения архитектуры системы

В.2.1 Общие положения

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

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

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

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

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

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

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

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

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

Модель представляет собой частный случай модели В.2.3, если период между контролями состояния системы больше периода прогноза. Учитывая это, используют формулы (В.1)—(В.5).

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

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

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

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

В рамках модели развитие событий в системе считается не нарушающим надежность реализации процесса определения архитектуры в течение заданного периода прогноза, если к началу этого периода требуемые условия для реализации процесса обеспечены и в течение всего периода либо источники угроз не активизируются, либо после активизации происходят их своевременное выявление и принятие адекватных мер противодействия угрозам. В целях моделирования предполагают, что существуют не только средства контроля (диагностики) состояния реализуемого процесса определения архитектуры, но и способы поддержания и/или восстановления возможностей по выполнению процесса при выявлении источников или следов активизации угроз. Восстановление осуществляется лишь в период системного контроля. Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии обеспечения надежности реализации процесса определения архитектуры системы из-за возможных угроз в течение периода прогноза (т. к. в принятой модели за счет предупреждающих действий по результатам диагностики устраняются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент нанесения ущерба от реализации какой-либо угрозы).

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

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

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

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

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

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;

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

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

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

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

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

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

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

Возможны два варианта:

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

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

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

Примечание — Формулу (В.2) используют также для оценки риска отсутствия нарушений надежности реализации процесса определения архитектуры системы при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по математической модели «черного ящика» при отсутствии какого-либо контроля (см. В.2.2).

Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия нарушений надежности реализации процесса определения архитектуры системы в течение прогноза $T_{\text{зад}}$ вычисляют по формуле

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

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

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

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

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

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

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

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

Формула (В.3) логически интерпретируется так: для обеспечения выполнения требований по защите информации за весь период прогноза требуется обеспечение выполнения требований по реализации процесса на каждом из участков — будь то середина или конец задаваемого периода прогноза $T_{\text{зад}}$.

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

В итоге вероятность отсутствия нарушений надежности реализации процесса определения архитектуры системы 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 определения архитектуры системы $P_{надежн}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{зад}$) в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по обеспечению выполнения процесса. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения надежности реализации процесса определения архитектуры системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

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

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

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

Расчет основан на применении следующих инженерных способов.

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

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

- для системы из двух последовательно соединенных элементов

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

- для системы из двух параллельно соединенных элементов

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

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

Рекурсивное применение соотношений (В.6), (В.7) снизу-вверх дает соответствующие вероятностные оценки для 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 систем-

ных элементов, представляемых в виде «черного ящика» в принятой сложной логической структуре системы, затем, учитывая характер логического объединения («И» или «ИЛИ») в принятой структуре, по формулам (В.6) или (В.7) проводится расчет вероятности нарушения надежности реализации процесса за время t для объединяемых подсистем. И так — до объединения на уровне системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (В.6) или (В.7) от исходных параметров моделей В.2.2 и В.2.3.

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

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

- 1-я итерация определяет $T^{(1)}_{диаг} = T_{диаг}$, 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

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

где $R^{(1)}$ — риск нарушения надежности реализации процесса с исходным значением $T^{(1)}_{диаг}$, вычисляемый с использованием модели В.2.3. Здесь, поскольку на 1-й итерации $T^{(1)}_{диаг}$ 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

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

где $R^{(r-1)}$ вычисляют по моделям В.2.2, В.2.3, но в качестве исходного уже выступает $T^{(r-1)}_{диаг}$, 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 $T^{(r)}_{диаг}$ сходится, и для дальнейших расчетов используют значение, отличающееся от точного предела $T^{(\infty)}_{диаг}$ на величину, пренебрежимо малую по сравнению с задаваемой изначально точностью итерации ε:

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

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

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

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

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

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

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

В.3.1 Общие положения

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

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

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

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

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

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

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

В.3.2 Исходные данные и расчетные показатели

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

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

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

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

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

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

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

Расчетные показатели:

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

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

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

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

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

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

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

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

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

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса определения архитектуры системы

Г.1 Общие положения

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

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

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

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

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

Г.1.3 Применительно к моделируемой системе для прогнозирования рисков определению подлежат:

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

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

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

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

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

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

Г.2 Цель прогнозирования рисков

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

Г.3 Положения по формализации

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

Г.3.2 В зависимости от целей прогнозирования рисков моделируемая система (см. приложение В) логически может быть представлена в виде «черного ящика» или в виде сложной структуры. Для отдельных элементов

сложной системы или при ее огрубленном моделировании используют модель «черного ящика». Для получения более точных результатов прогнозирования рисков осуществляют декомпозицию сложной моделируемой системы до уровня составных системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых для описания целостности системы логическими условиями «И», «ИЛИ» (см. В.2.4).

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

- «Надежность реализации процесса определения архитектуры «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены «И» надежность выполнения определенных действий процесса для получения выходных результатов, «И» выполнение определенных требований по защите информации;

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

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

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

- «Выполнение требований по защите информации в процессе определения архитектуры нарушено» — в противном случае.

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

В Г.7 приведены примеры прогнозирования рисков.

Г.4 Показатели, исходные данные и расчетные соотношения

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

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

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

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

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

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

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

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

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

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

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

Г.6 Обработка и использование результатов прогнозирования

Результаты прогнозирования рисков должны быть удобны для обработки заказчиком системного анализа и/или аналитиком моделируемой системы. Результаты представляются в виде гистограмм, графиков, таблиц и/или в ином виде, позволяющем анализировать зависимости рисков от изменения значений исходных данных при

решении задач системного анализа. Результаты расчетов подлежат использованию для решения задач системного анализа — см. раздел 7, приложение Е и ГОСТ Р 59349.

Г.7 Примеры

Г.7.1 Приведенные примеры демонстрируют отдельные аналитические возможности методических указаний. Пусть некоторое предприятие опасного производства формирует комплекс архитектурных решений согласно рекомендациям ГОСТ Р ИСО 15704 по общей стандартной архитектуре предприятия. Отдельно определяют:

- архитектурно-организационные решения, ориентированные на человека;
- архитектурные решения, ориентированные на процессы;
- архитектурные решения, ориентированные на применяемые технологии.

В рамках примеров, не вдаваясь в детали рассматриваемых архитектур, осуществляется системный анализ структуры комплекса архитектурных решений, представленной на рисунке Г.1.

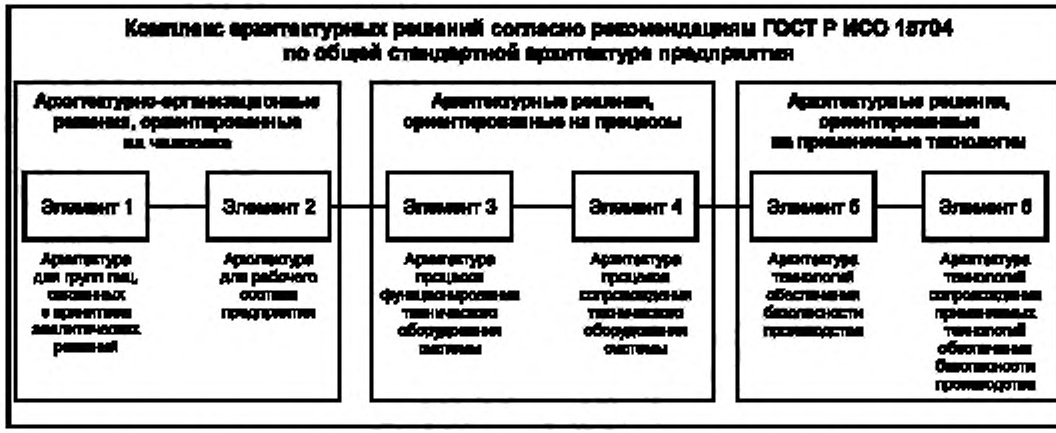

Рисунок Г.1 — Структура моделируемой системы в виде комплекса архитектурных решений

Именно эта структура является в примерах моделируемой системой. Элементами моделируемой системы являются:

- в рамках архитектурно-организационных решений, ориентированных на человека:

1-й элемент — архитектура для группы лиц, связанных с принятием аналитических решений (для руководителей, проектировщиков, конструкторов, инженеров, аналитиков, интеграторов),

2-й элемент — архитектура для рабочего состава предприятия (для мастеров, техников, механиков, операторов, водителей, обслуживающего персонала, бухгалтерии);

- в рамках архитектурных решений, ориентированных на процессы:

3-й элемент — архитектура процесса функционирования технического оборудования системы,

4-й элемент — архитектура процесса сопровождения технического оборудования системы;

- в рамках архитектурных решений, ориентированных на применяемые технологии:

5-й элемент — архитектура технологий обеспечения безопасности производства,

6-й элемент — архитектура технологий сопровождения применяемых технологий обеспечения безопасности производства.

По определению надежность реализации процесса определения архитектуры моделируемой системы считается обеспеченной в течение заданного периода прогноза, если в течение этого периода надежно выполнены действия процесса «И» по архитектурно-организационным решениям, ориентированным на человека (по 1-му и 2-му элементам), «И» по архитектурным решениям, ориентированным на процессы (по 3-му и 4-му элементам), «И» по архитектурным решениям, ориентированным на применяемые технологии (по 5-му и 6-му элементам), причем эти архитектурные решения будут приемлемыми в течение такого же периода и в будущем (при эксплуатации моделируемой системы). То есть сам период прогноза для отдельного элемента может быть интерпретирован как относящийся и к стадии создания (по угрозам, свойственным этой стадии), и к стадии эксплуатации в будущем (по потенциально возможным угрозам), моделируя приемлемость архитектурных решений и подтверждение гарантий удержания рисков в допустимых пределах.

С учетом возможных ущербов цели прогнозирования рисков сформулированы руководством предприятия следующим образом.

Цели — в условиях существующей неопределенности:

- количественно оценить риски нарушения надежности реализации процесса определения архитектуры предприятия без учета требований по защите информации (как поэлементно, так и для комплекса архитектурных решений);

- количественно оценить риски нарушения требований по защите информации (как поэлементно, так и для комплекса архитектурных решений);

- количественно оценить риски нарушения надежности реализации процесса определения архитектуры предприятия с учетом требований по защите информации (целиком для всего комплекса архитектурных решений);

- определить такой период, при котором сохраняются гарантии удержания рисков в допустимых пределах;

- определить критичные условия в развитии различных угроз.

Тем самым выполнены шаги 1, 2 настоящих методических указаний.

Пример 1 посвящен прогнозированию риска нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации, пример 2 посвящен прогнозированию риска нарушения требований по защите информации, пример 3 иллюстрирует прогнозирование интегрального риска нарушения реализации процесса определения архитектуры системы с учетом требований по защите информации.

Г.7.2 Пример 1. Прогнозирование риска нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации проиллюстрировано для моделирования комплекса архитектурных решений, представленных на рисунке Г.1. Выполняя шаг 3, выявлены возможные угрозы, критично влияющие на безопасность каждого из структурных элементов моделируемой системы. При этом учтены угрозы, связанные не только с причинами человеческих ошибок на уровнях принятия решений при определении архитектуры, но и гипотетичные угрозы, связанные с последствиями этих ошибок на этапе функционирования предприятия. Сформированные исходные данные по каждому из 6 составных элементов представлены в таблице Г.1.

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

Исходные данные	Значения и комментарии		
	для 1-го/2-го элементов	для 3-го/4-го элементов	для 5-го/6-го элементов
σ — частота возникновения источников угроз нарушения надежности реализации процесса для элемента	1 раз в год/1 раз в год (из-за недостаточной квалификации, компетенции или знаний для решения задач или из-за проблем со здоровьем персонала) — это угрозы, связанные с причинами человеческих ошибок на уровнях принятия решений/рабочей реализации решений в системе	1 раз в год (что соизмеримо со временем наработки на отказ оборудования)/1 раз в 5 лет (что объясняется редкими сбоями в процессе сопровождения оборудования системы) — это угрозы ущерба в процессах функционирования/сопровождения системы (кроме угроз нарушения технологической безопасности)	1 раз в 2 года (что соизмеримо со временем наработки на технологический отказ)/1 раз в 5 лет (что объясняется редкими сбоями в процессе сопровождения технологической безопасности системы) — это угрозы возникновения ущерба при нарушении технологической безопасности системы
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 архитектурные решения)/5 лет (что соизмеримо со временем между критичными ошибками в рабочей реализации решений) — это означает, что развитие угроз может привести к последующим ущербам из-за человеческих ошибок на уровнях принятия решений/рабочей реализации решений в системе	12 мес (что соизмеримо со временем постепенного отказа оборудования системы с учетом технического обслуживания)/6 мес (что объясняется сохранением минимальных возможностей системы функционировать в устаревшей среде без обновлений, осуществляемых при сопровождении) — это время до ущерба после возникновения признаков угроз для процессов функционирования/сопровождения системы (кроме угроз нарушения технологической безопасности)	1 мес (что соизмеримо со временем постепенного технологического отказа системы с учетом технического обслуживания)/6 мес (что объясняется сохранением минимальных возможностей системы функционировать в устаревшей среде без обновлений, осуществляемых при сопровождении) — это время до ущерба после возникновения признаков угроз нарушения технологической безопасности системы

Окончание таблицы Г.1

Исходные данные	Значения и комментарии		
	для 1-го/2-го элементов	для 3-го/4-го элементов	для 5-го/6-го элементов
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей элемента	8 ч/8 ч — определяется регламентом контроля готовности персонала к работе — 1 раз за смену (при 8-часовом рабочем дне)	1 ч/1 мес — определяется регламентом контроля процесса функционирования/контроля процесса сопровождения системы (кроме контроля технологической безопасности)	1 ч/1 мес — определяется регламентом контроля технологической безопасности производства/контроля процесса сопровождения технологической безопасности системы
$T_{диаг}$ — среднее время диагностики состояния элемента	10 мин/10 мин — определяется временем медицинского обследования перед работой	30 с/30 с — автоматический контроль целостности оборудования/контроль процесса сопровождения оборудования системы	30 с/30 с — автоматический контроль технологической безопасности/контроль процесса сопровождения технологической безопасности системы
$T_{восст}$ — среднее время восстановления элемента после выявления нарушений	1 ч/1 ч — это время замены человека, отстраненного от выполнения обязанностей, и возложения необходимых функциональных обязанностей на заменяющего человека	30 мин (включая перезагрузку программного обеспечения оборудования)/1 нед (включая поиск новых подрядчиков для сопровождения системы)	1 сут (включая восстановление технологического производства)/1 нед (включая поиск новых подрядчиков для сопровождения системы)
$T_{зад}$ — задаваемый период прогноза	От полугода до 2 лет (для определения периода времени, при котором сохраняются гарантии удержания риска в допустимых пределах)		

При выполнении шага 4 прогнозирование риска нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации осуществлено с использованием расчетных соотношений (В.1)—(В.9) согласно рекомендациям В.2.2 и В.2.3.

Анализ результатов моделирования показал, что в вероятностном выражении риск нарушения надежности реализации процесса определения архитектуры моделируемой системы без учета требований по защите информации в течение года (т. е. для периода прогноза, равного 12 мес) составит за весь комплекс архитектурных решений около 0,040 (см. рисунок Г.2), составляя для 1-го элемента — 0,012, для 4-го и 6-го элементов — 0,014, для 2-го, 3-го и 5-го элементов — не превышает 0,0001. При увеличении периода прогноза от полугода до 2 лет риск возрастает от 0,018 до 0,083 (см. рисунок Г.3). Для допустимого риска на уровне 0,05 обоснован период до 15 мес, при котором сохраняются гарантии удержания риска в допустимых пределах в выбранных архитектурных решениях, характеризуемых условиями примера из таблицы Г.1.

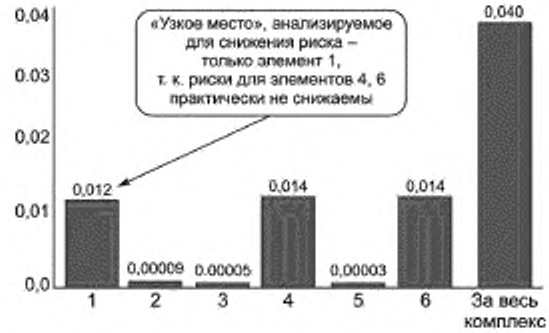

Рисунок Г.2 — Оценки риска нарушения надежности реализации процесса определения архитектуры без учета требований по защите информации в течение года

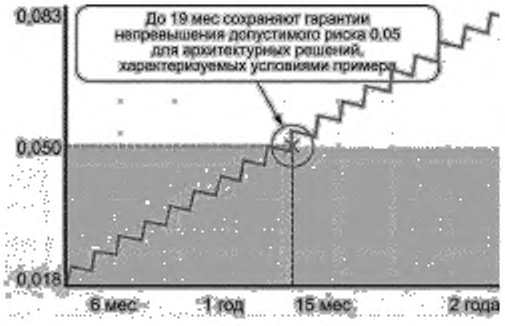

Рисунок Г.3 — Зависимость риска от периода прогноза длительностью от 6 до 24 мес

При этом «узким» местом, характеристики которого необходимо анализировать на предмет снижения риска, является лишь 1-й элемент — это архитектура для группы лиц, связанных с принятием аналитических решений (для руководителей, проектировщиков, конструкторов, инженеров, аналитиков, интеграторов). Выявление этого «узкого» места становится причиной проведения дополнительного системного анализа на предмет снижения риска. Самым простым вариантом является объединение усилий в решении одной и той же задачи со стороны нескольких лиц, связанных с принятием аналитических решений. Эти усилия подразумевают взаимный контроль и согласование деятельности, а с точки зрения моделирования в структуре вместо 1-го элемента появляется 1-я подсистема, представляемая в виде двух параллельно объединяемых элементов. Все исходные данные для каждого из параллельно объединенных элементов 1-й подсистемы такие же, как и для 1-го элемента из таблицы Г.1. В итоге дополнительного моделирования установлено: за счет предпринятых мер обосновано снижение на 42 % риска нарушения надежности реализации процесса определения архитектуры без учета требований по защите информации и увеличение на 27 % периода, для которого сохраняются гарантии удержания риска в допустимых пределах (с 25 до 19 мес — см. рисунок Г.4).

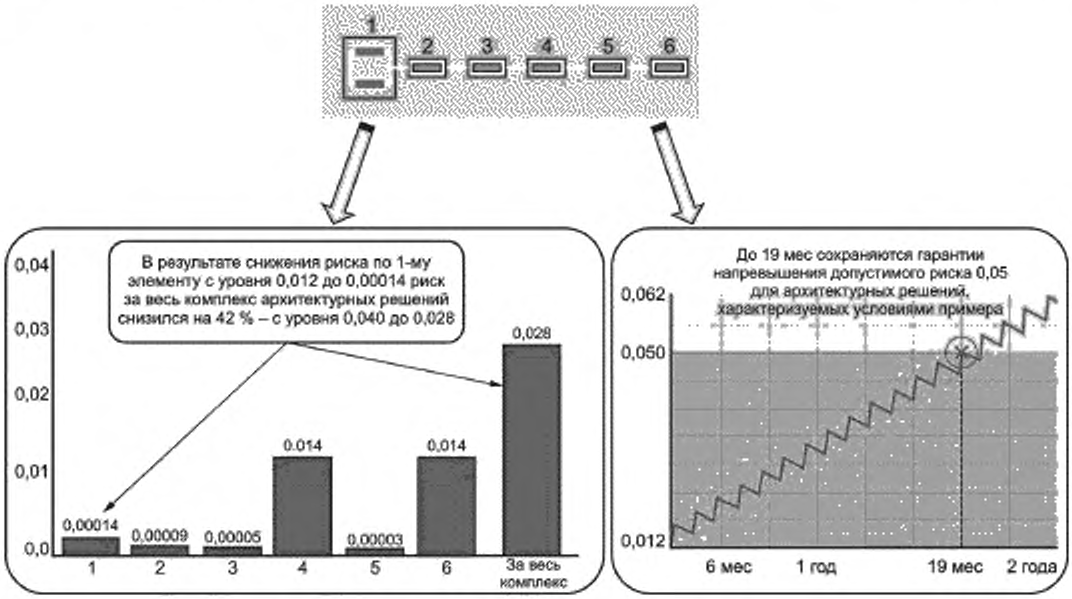

Рисунок Г.4 — Риск нарушения надежности реализации процесса определения архитектуры без учета требований по защите информации снижается, а период, для которого сохраняются гарантии удержания риска в допустимых пределах, увеличивается

На практике именно эти меры (объединение усилий нескольких лиц в параллельном решении одной задачи с взаимным контролем и согласованием подготавливаемых решений) приводят к надежной реализации рассматриваемого процесса. В примере представлена лишь количественная оценка подобных мер в терминах прогнозируемых рисков (по каждому элементу).

Г.7.3 Пример 2. В продолжение примера 1 прогнозирование риска нарушения требований по защите информации проиллюстрировано для комплекса архитектурных решений согласно рекомендациям ГОСТ Р ИСО 15704 по общей стандартной архитектуре предприятия. Осуществлена привязка требований (например, по ГОСТ Р ИСО/МЭК 27001) к структуре комплекса архитектурных решений, аналогичной структуре, рассмотренной в примере Г.7.2 (см. рисунок Г.5). При этом учтены угрозы, связанные не только с причинами неадекватного учета требований по защите информации на уровнях принятия решений при определении архитектуры, но и гипотетичные угрозы, связанные с последствиями этого неадекватного учета на этапе функционирования предприятия. Исходные данные по каждому из 6 составных элементов представлены в таблице Г.2. Прогнозирование риска нарушения требований по защите информации осуществлено с использованием рекомендаций В.3.

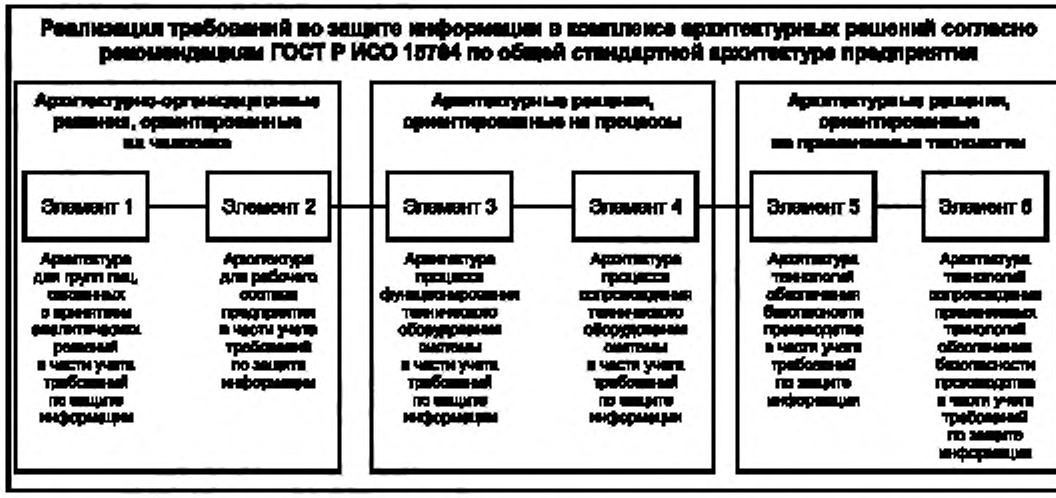

Рисунок Г.5 — Структура моделируемой системы в виде комплекса архитектурных решений в части учета требований по защите информации

Таблица Г.2 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе определения архитектуры системы

Исходные данные	Значения и комментарии		
	для 1-го/2-го элементов	для 3-го/4-го элементов	для 5-го/6-го элементов
σ — частота возникновения источников угроз нарушения требований по защите информации	1 раз в год/1 раз в год (угрозы, связанные с субъективными факторами)	1 раз в год (что соизмеримо со временем наработки на отказ оборудования)/1 раз в 5 лет (что объясняется маскировкой под редкие сбои в процессе сопровождения оборудования системы) — это угрозы ущерба в процессах функционирования/сопровождения системы (кроме угроз нарушения технологической безопасности)	1 раз в 2 года (что соизмеримо со временем наработки на технологический отказ)/1 раз в 5 лет (что объясняется маскировкой под нарушения технологической безопасности в процессе сопровождения системы) — это угрозы возникновения ущерба при нарушении технологической безопасности системы

Окончание таблицы Г.2

Исходные данные	Значения и комментарии		
	для 1-го/2-го элементов	для 3-го/4-го элементов	для 5-го/6-го элементов
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	2 нед (что соизмеримо со временем использования уязвимостей в архитектурных решениях в части защиты информации/5 лет (что соизмеримо со временем между критичными ошибками со стороны рабочего состава, связанными с нарушением требований по защите информации) — это возможное время до ущерба от нарушения требований по защите информации в архитектурных решениях	1 сут/1 сут (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее 1 сут) — это время до ущерба после возникновения признаков угроз для процессов функционирования/сопровождения системы (кроме угроз нарушения технологической безопасности)	1 сут/1 сут (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой не менее 1 сут) — это время до ущерба после возникновения признаков угроз нарушения технологической безопасности производства/и сопровождения технологической безопасности системы
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	1 сут/1 сут — определяется регламентом контроля целостности программного обеспечения и активов, относящихся к персоналу предприятия и используемых в процессе функционирования/сопровождения системы	1 ч/1 ч — определяется регламентом контроля целостности программного обеспечения и активов, используемых в процессе функционирования/и сопровождения системы	1 ч/1 ч — определяется регламентом контроля целостности программного обеспечения и активов, используемых для технологической безопасности производства/и сопровождения технологической безопасности системы
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы защиты информации	30 с/30 с — автоматический контроль целостности программного обеспечения и активов, относящихся к персоналу предприятия	30 с/30 с — автоматический контроль целостности программного обеспечения и активов, используемых в процессе функционирования/и сопровождения системы	30 с/30 с — автоматический контроль целостности программного обеспечения и активов, используемых для технологической безопасности производства/ и сопровождения технологической безопасности системы
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	5 мин/5 мин (включая перезагрузку программного обеспечения и восстановление персональных данных)	5 мин/5 мин (включая перезагрузку программного обеспечения и восстановление данных)	5 мин/5 мин (включая перезагрузку программного обеспечения и восстановление данных)
$T_{зад}$ — задаваемая длительность периода прогноза	От 6 мес до 2 лет (для определения периода, при котором сохраняются гарантии удержания риска в допустимых пределах для обеспечения нормы эффективности защиты информации)		

Анализ результатов моделирования показал, что в вероятностном выражении риск нарушения требований по защите информации в течение года составит за весь комплекс архитектурных решений около 0,071 (см. рисунок Г.6), составляя для 1-го элемента — 0,034 («узкое» место), для 3-го элемента — 0,021, для 2-го, 4-го, 5-го и 6-го элементов — не превышает 0,010. При увеличении периода прогноза от полугода до 2 лет риск возрастает от 0,040 до 0,140 (см. рисунок Г.7). Для допустимого риска на уровне 0,05 обоснован период до 8 мес, при котором сохраняются гарантии удержания риска в допустимых пределах в выбранных архитектурных решениях, характеризуемых условиями примера из таблицы Г.2.

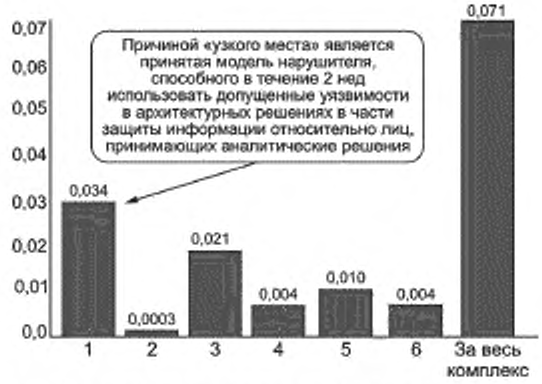

Рисунок Г.6 — Оценки риска нарушения требований по защите информации в течение года

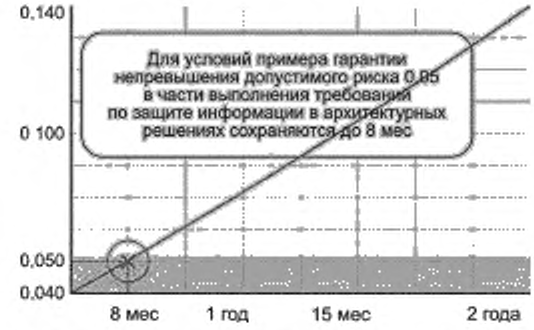

Рисунок Г.7 — Зависимость риска от периода прогноза длительностью от 6 до 24 мес

«Узкое» место представляют собой допущенные уязвимости в архитектурных решениях в части защиты информации относительно лиц, принимающих аналитические решения (1-й элемент). При этом причиной «узкого» места является принятая модель нарушителя, способного в течение 2 нед использовать эти гипотетичные уязвимости.

Г.7.4 Пример 3. В продолжение примеров 1 и 2 интегральный риск $R_{интегр}(T_{зад})$ нарушения надежности реализации процесса определения архитектуры системы с учетом требований по защите информации рассчитан с использованием рекомендаций В.4.

Учитывая, что период прогноза $T_{зад} = 1$ год, по результатам примера 1 $R_{надежн}(T_{зад}) = 0,028$, а по результатам примера 2 $R_{наруш}(T_{зад}) = 0,071$, по формуле (В.10)

$$R_{интегр}(T_{зад}) = 1 - (1 - 0,028) \cdot (1 - 0,071) \approx 0,097.$$

В итоге интегральный риск нарушения реализации процесса определения архитектуры системы в течение 1 года с учетом требований по защите информации составит около 0,097. При этом риск нарушения требований по защите информации (0,071) в 2,5 раза превышает риск нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации. Сравнивая с рекомендациями приложения Д, можно констатировать превышение расчетных рисков по сравнению с допустимым уровнем риска, т. е. обоснована потребность улучшения архитектурных решений (в первую очередь для уменьшения риска нарушения требований по защите информации). Новые архитектурные решения также подлежат системному анализу с использованием прогнозирования рисков.

Тем самым продемонстрированы отдельные аналитические возможности методов и моделей стандарта (см. приложение В), 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 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59356.

Г.8 Материально-техническое обеспечение

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

- результаты обследования, концепция создания, технический облик и/или ТЗ на разработку для создаваемой системы, конструкторская и эксплуатационная документация для существующей системы (используют для формирования исходных данных при моделировании);
- модель угроз безопасности информации (используют для формирования необходимых исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- записи из системного журнала учета предпосылок, инцидентов и аварий при функционировании системы, связанных с нарушением требований по защите информации (используют для формирования исходных данных при моделировании);
- планы ликвидации нарушений, инцидентов и аварий, связанных с нарушением требований по защите информации, и восстановления целостности системы (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- обязанности должностных лиц и инструкции по защите информации при выполнении процесса (используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- программные комплексы, поддерживающие применение математических моделей и методов по настоящим методическим указаниям (используют для проведения расчетов и поддержки процедур системного анализа и принимаемых решений).

Г.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 определения архитектуры системы

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

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

Требования системной инженерии при допустимых рисках, свойственных конкретной системе или ее аналогу и 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 определения архитектуры системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

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

Таблица Д.1 — Пример задания допустимых значений рисков

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

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса определения архитектуры системы

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

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

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

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

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

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

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утверждены приказом Председателя Гостехкомиссии России от 30 августа 2002 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, архитектура, безопасность, защита информации, модель, процесс определения архитектуры системы, риск, системная инженерия, управление

Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 11.05.2021. Подписано в печать 20.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21.

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 tinfo.ru

gost.e-ecolog.ru