ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59331— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ 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 28 апреля 2021 г. № 307-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе управления инфраструктурой системы 8
5 Общие требования системной инженерии по защите информации в процессе управления инфраструктурой системы 9
6 Специальные требования к количественным показателям 11
7 Требования к системному анализу 13
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 управления инфраструктурой системы 24
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса управления инфраструктурой системы 36
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса управления инфраструктурой системы 37
Библиография 38

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 портфелем, управления человеческими ресурсами, управления качеством, управления знаниями — по ГОСТ Р 59330, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335. Для процесса управления инфраструктурой системы — по настоящему стандарту;

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

- для технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357.

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ СИСТЕМЫ

System engineering. Protection of information in system infrastructure management process

Дата введения — 2021—11—30

1 Область применения

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

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

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

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процесс управления инфраструктурой системы, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем, — см. примеры систем в [1]—[27].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

Издание официальное

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

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

ГОСТ 32867 Дороги общего пользования. Организация строительства. Общие требования

ГОСТ 34059 Инженерные сети зданий и сооружений внутренние. Устройство систем отопления, горячего и холодного водоснабжения. Общие технические требования

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 10.0.05—2019/ИСО 12006-2:2015 Система стандартов информационного моделирования зданий и сооружений. Строительство зданий. Структура информации об объектах строительства. Часть 2. Основные принципы классификации

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

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 27005—2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 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 51901.7/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 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

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

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

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

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

ГОСТ Р 56425 Технопарки. Требования

ГОСТ Р 56923/ISO/IEC TR 24748-3:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 3. Руководство по применению ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

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

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

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

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

ГОСТ Р 58812 Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация

ГОСТ Р 59215 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий

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

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

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

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

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

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

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

ГОСТ Р 59337 Системная инженерия. Защита информации в процессе оценки и контроля проекта

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 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 Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ 32867, ГОСТ 34059, ГОСТ Р 51897, ГОСТ Р 58811, ГОСТ Р 58812, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

актив: Что-либо, что имеет ценность для организации.

Примечание — Имеются различные типы активов:
- информация;
- программное обеспечение;
- материальные активы, например, компьютер;
- услуги;
- люди и их квалификация, навыки и опыт;
- нематериальные активы, такие как репутация и имидж.

[ГОСТ Р ИСО/МЭК 27000—2012, пункт 2.3]

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

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]

3.1.4

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]

3.1.5

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]

3.1.6

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]

3.1.7

инновационная инфраструктура: Совокупность организаций, образующих инфраструктуру поддержки субъектов малого и среднего предпринимательства в научно-технологической сфере, в том числе бизнес-инкубаторы, региональные центры инжиниринга, центры сертификации, стандартизации и испытаний и иные организации, обеспечивающие коммерциализацию результатов научно-технических исследований и разработок.

[ГОСТ Р 56425—2015, пункт 3.9]

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

3.1.9

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

[ГОСТ Р 53114—2008, статья 3.1.4]

3.1.10 **инфраструктура системы:** Комплекс взаимосвязанных объектов, структур и элементов, составляющих и обеспечивающих основу создания и/или эксплуатации системы согласно ее целевому назначению и/или выведению системы из эксплуатации.

Примечание — В общем случае инфраструктуру современной системы образуют здания, сооружения, оборудование, программно-аппаратная среда и службы обеспечения, необходимые для создания (модернизации, развития) и/или эксплуатации системы, и/или выведения системы из эксплуатации. Например, инфраструктура системы, представляющей собой научно-производственную организацию, может включать в себя технопарк, состоящий из технологической инфраструктуры (зданий, сооружений, строительного комплекса), инженерной инфраструктуры (сооружения связи, в том числе линейно-кабельных сооружений), коммунальной инфраструктуры (систем горячего и холодного водоснабжения, отопления, теплоснабжения, теплопотребления, теплового пункта, канализации), центра обработки данных (ЦОД), телекоммуникационных сетей, систем хранения и передачи данных, системы поддержки принятия решений, инновационной инфраструктуры для научно-технических исследований и разработок, транспортной инфраструктуры, системы обеспечения безопасности.

3.1.11

коммунальная инфраструктура: Система коммуникаций и объектов водоснабжения, водоотведения, теплоснабжения, электроэнергетики, электроснабжения и газоснабжения, связи, обеспечивающая функционирование технопарка.

[ГОСТ Р 56425—2015, пункт 3.5]

3.1.12 **надежность реализации процесса управления инфраструктурой системы:** Свойство процесса сохранять во времени в установленных пределах значения показателей процесса, характеризующих способность выполнить процесс в заданных условиях его реализации.

3.1.13

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.14

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.15

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.
[ГОСТ Р 51898—2002, пункт 3.2]

3.1.16

система: Комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей.

Примечания

1 Система может рассматриваться как какой-то продукт или как предоставляемые услуги, обеспечивающие этот продукт.

2 На практике, интерпретация данного термина зачастую уточняется с помощью ассоциативного существительного, например, система самолета. В некоторых случаях слово система может заменяться контекстно зависимым синонимом, например, самолет, хотя это может впоследствии затруднить восприятие системных принципов.

[ГОСТ Р 57193—2016, пункт 4.1.44]

3.1.17 **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 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.

3.1.18

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]

3.1.19

строительный комплекс: Совокупность одного или более строительных сооружений, предназначенных для обеспечения выполнения как минимум одной функции или деятельности пользователя.

Примечание — Строительный комплекс можно разделить на составляющие элементы и идентифицировать строительные сооружения, которые его образуют; например, аэропорт обычно состоит из таких строительных сооружений, как взлетно-посадочная полоса, диспетчерская башня, здание терминала, ангара для самолетов и др. Бизнес-парк обычно состоит из некоторого количества зданий, подъездных дорог и объектов ландшафтной архитектуры (каждый из которых представляет собой отдельное строительное сооружение). Автомагистраль, ведущая из точки А в точку В, состоит из сервисных станций, дорожного покрытия, мостов, насыпей, объектов ландшафтной архитектуры и др.

[ГОСТ Р 10.0.05—2019/ИСО 12006-2:2015, пункт 3.4.1]

3.1.20

технологическая инфраструктура: Комплекс специализированного оборудования, предназначенного для оснащения лабораторий, вивариев, инновационно-технологических центров, центров промышленного дизайна, центров прототипирования, центров трансфера технологий и иных объектов, необходимых резидентам для ведения хозяйственной деятельности на территории технопарка.
[ГОСТ Р 56425—2015, пункт 3.10]

3.1.21

технопарк: Управляемый управляющей компанией комплекс объектов коммунальной, транспортной и технологической инфраструктуры, обеспечивающий полный цикл услуг по размещению и развитию инновационных компаний, являющихся резидентами технопарка.
[ГОСТ Р 56425—2015, пункт 3.1]

3.1.22

транспортная инфраструктура: Совокупность объектов недвижимого имущества технопарка, предназначенная для обеспечения движения транспортных средств резидентов технопарка, в том числе автомобильных дорог, железнодорожных путей, портов, тоннелей, эстакад, мостов, переездов, путепроводов.

[ГОСТ Р 56425—2015, пункт 3.7]

3.1.23

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

[ГОСТ Р 50922—2006, статья 2.9.2]

3.1.24

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

3.1.25

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использованы следующие сокращения:

ТЗ — техническое задание;

ЦОД — центр обработки данных.

4 Основные положения системной инженерии по защите информации в процессе управления инфраструктурой системы

4.1 Общие положения

Организации используют процесс управления инфраструктурой системы для того, чтобы преобразовать представление заинтересованных сторон о желательных возможностях системы в технические решения, соответствующие эксплуатационным потребностям пользователей. В процессе управления инфраструктурой 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 этих рисков или их удержанию в допустимых пределах используют системный анализ процесса с учетом требований по защите информации.

Определение выходных результатов процесса управления инфраструктурой системы и типовых действий по защите информации осуществляют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ 32867, ГОСТ 34059, ГОСТ Р 10.0.05, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53114, ГОСТ Р 53647.1, ГОСТ Р 56425, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58494, ГОСТ Р 58811, ГОСТ Р МЭК 62264-1. Оценку интегрального риска нарушения реализации процесса с учетом требований по защите информации 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 51901.7, ГОСТ Р 54124, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355. При этом учитывают специфику системы — см., например, [20]—[27].

4.2 Цель процесса управления инфраструктурой системы и назначение мер защиты информации

4.2.1 Определение целей процесса управления инфраструктурой системы осуществляют по ГОСТ Р 10.0.05, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085,

ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 53114, ГОСТ Р 53647.1, ГОСТ Р 56425, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58811, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики системы.

В общем случае главной целью процесса управления инфраструктурой системы является поддержка таких проектных и эксплуатационных решений и действий, выполнение которых формирует функциональные возможности для создания (модернизации, развития) и/или эксплуатации системы и/или выведения системы из эксплуатации. Процесс управления инфраструктурой системы определяет, обеспечивает и поддерживает активы основных средств, инструментарии, связи и информационные технологии, необходимые для бизнеса организации.

4.2.2 Меры защиты информации в процессе управления инфраструктурой системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, [20] — [24] с учетом специфики рассматриваемой системы и реализуемой стадии ее жизненного цикла.

4.3 Стадии и этапы жизненного цикла системы

Процесс управления инфраструктурой системы может быть использован на любой стадии жизненного цикла системы. Стадии и этапы работ устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 53622, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58811, [21]—[24].

Процесс управления инфраструктурой системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.4 Основные принципы

При проведении системного анализа процесса управления инфраструктурой 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 по обеспечению защиты информации в процессе управления инфраструктурой системы

Основные усилия системной инженерии по обеспечению защиты информации в процессе управления инфраструктурой 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 управления инфраструктурой 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 каковой 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 управления инфраструктурой 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 соглашений.

Примечания

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

2 При использовании процесса управления инфраструктурой в системах искусственного интеллекта необходимо гарантированно подтверждать достаточность автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации), учитывать возможность повышения уровня конфиденциальности данных в процессе их обработки системами 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 призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации процесса управления инфраструктурой системы и по поддержке при этом эффективности защиты информации.

Требования системной инженерии по защите информации в процессе управления инфраструктурой системы включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе управления инфраструктурой системы определяют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ 32867, ГОСТ 34059, ГОСТ IEC 61508-3, ГОСТ Р 10.0.05, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53114, ГОСТ Р 53647.1, ГОСТ Р 56425, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58494, ГОСТ Р 58811, ГОСТ Р 59215, ГОСТ Р МЭК 62264-1 с учетом специфики системы.

5.4 Меры защиты информации и действия по защите информации должны охватывать активы, информация которых или о которых подлежит защите для получения выходных результатов и выполнения процесса управления инфраструктурой системы.

Примечание — В состав активов могут быть включены активы, используемые для достижения целей управления инфраструктурой для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика, — например, для систем и средств контроля надежности инфраструктуры.

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 56923, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62264-1 и специфики системы (см., например, [20]—[27]).

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

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

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, [21]—[26].

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

Качественные показатели для оценки рисков в области информационной безопасности определены в ГОСТ Р ИСО/МЭК 27005. Целесообразность использования количественных показателей рисков в дополнение к качественным показателям может потребовать дополнительного обоснования. Состав специальных количественных показателей рисков в интересах системного анализа процесса управления инфраструктурой системы определен в 6.3.

Типовые модели и методы системного анализа процесса управления инфраструктурой 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 рассматриваемым процессам и возможным условиям их реализации.

6 Специальные требования к количественным показателям

6.1 Общие положения

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

6.1.2 В общем случае основными выходными результатами процесса управления инфраструктурой системы являются:

- описание системы и применяемой инфраструктуры, включая взаимодействия системы и инфраструктурных (в т. ч. обеспечивающих) подсистем, их функции и границы;
- системные требования и проектные ограничения, включая функциональные, эксплуатационные, процессные требования и требования по взаимодействию системы и инфраструктурных (в т. ч. обеспечивающих) подсистем;
- материалы эскизного и/или технического проектирования системы;
- отчеты по анализу системных требований;
- требования к применяемой инфраструктуре системы и обеспечивающим системам или системным элементам, необходимым для выполнения действий процесса;
- элементы инфраструктуры системы, соответствующие требованиям, предъявляемым к системе;
- описание комплексов программных, программно-аппаратных и технических средств, определяющих инфраструктуру системы и ее применение;
- акты, протоколы, предписания с результатами контроля состояния инфраструктуры системы;
- график технического обслуживания (сопровождения) инфраструктуры системы;
- план мероприятий по охране труда (в части, качающейся инфраструктуры системы);
- инструкции по монтажу, пуску и регулированию элементов инфраструктуры системы;
- паспорт на инфраструктуру системы в целом и на отдельные инфраструктурные элементы (при необходимости);
- ведомость комплекта запасных частей, инструментов и принадлежностей;
- эксплуатационные и специальные инструкции;
- технические условия и требования на ремонт элементов инфраструктуры системы.

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

- определение проектных требований к инфраструктуре системы;

- выработку стратегии по созданию (модернизации) и развитию инфраструктуры системы;
- разработку технического задания на создание (модернизацию) или развитие инфраструктуры системы;
- разработку рабочей документации на инфраструктуру системы;
- определение элементов инфраструктуры системы, включая инструментарии, программные средства, программно-аппаратные и технические средства, услуги и стандарты;
- отбор элементов инфраструктуры системы, удовлетворяющих требованиям конкретного проекта;
- анализ соответствия отобранных элементов инфраструктуры системы требованиям конкретного проекта;
- приобретение необходимых элементов инфраструктуры системы;
- проведение сертификационных и аттестационных испытаний элементов инфраструктуры системы (при необходимости);
- техническое обслуживание (сопровождение) и необходимую поддержку инфраструктуры системы, включая:
  - выполнение работ для поддержания инфраструктуры системы в работоспособном состоянии,
  - оценку степени, до которой элементы инфраструктуры системы и поставленные инфраструктурные ресурсы удовлетворяют требованиям проекта,
  - определение и обеспечение улучшений или изменений по инфраструктурным ресурсам, включая при необходимости изменения требований проекта;
- оценку рисков нарушения надежности реализации процесса управления инфраструктурой системы;
- оценку эффективности функционирования системы с использованием процесса управления инфраструктурой системы.

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

6.2 Требования к составу показателей

Выбираемые показатели должны обеспечивать проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения реализации процесса управления инфраструктурой 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 в процессе управления инфраструктурой системы используют следующие количественные показатели:
- риск нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации;
- риск нарушения требований по защите информации в процессе управления инфраструктурой системы;
- интегральный риск нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации.

6.3.2 Риск нарушения надежности реализации процесса управления инфраструктурой 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 управления инфраструктурой 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 предъявлены определенные требования по защите информации.

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

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессу управления инфраструктурой 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 управления инфраструктурой системы включают в себя:

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

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

При обосновании и формулировании конкретных требований к системному анализу процесса управления инфраструктурой системы дополнительно руководствуются рекомендациями 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 17359, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы (см., например, [21]—[27]).

Примечание — Примеры решения задач системного анализа в приложении к различным процессам см. в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе управления инфраструктурой 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. [21]—[24];
- договоры и соглашения на проведение работ, связанных с инфраструктурой системы;
- лицензии, подтверждающие право поставщика (производителя) на проведение работ, связанных с инфраструктурой системы;
- финансовые и плановые документы на проведение работ, связанных с инфраструктурой системы;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- документацию при выполнении научно-исследовательских работ, связанных с инфраструктурой системы, — по ГОСТ 7.32, ГОСТ 15.101;
- конструкторскую и технологическую документацию, связанную с инфраструктурой системы, — по ГОСТ 2.051, ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201;
- эксплуатационную и ремонтную документацию — по ГОСТ 2.602, ГОСТ 34.201, ГОСТ Р 2.601 с учетом специфики системы;
- документацию системы менеджмента качества организации — по ГОСТ Р ИСО 9001;
- ТЗ — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839 с учетом специфики системы;
- персональные данные, базу данных и базу знаний, систему хранения архивов;
- систему передачи данных и облачные данные организации;
- выходные результаты иных процессов в жизненном цикле системы с учетом ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе управления инфраструктурой 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 ИСО/МЭК 27036-2, ГОСТ Р 51275, ГОСТ Р 59215;

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

- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124;

- угрозы безопасности информации при подготовке и обработке документов, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412;

- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С;

- угрозы компрометации информационной безопасности приобретающей стороны, угрозы возникновения ущерба репутации и/или потери доверия поставщика к конкретному заказчику, информация и информационные системы которого были скомпрометированы, — по ГОСТ Р 59215;

- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги, — по ГОСТ Р ИСО/МЭК 27036-4;

- угрозы, связанные с неопределенностью ответственности за обеспечение защиты информации в процессе управления инфраструктурой системы:

- 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 управления инфраструктурой системы применяют любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. С учетом набираемой статистики в настоящем стандарте типовые модели и методы системного анализа обеспечивают оценку следующих показателей согласно 6.3:

- риска нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации — см. В.1.2 — В.1.9, В.2;

- риска нарушения требований по защите информации в процессе управления инфраструктурой системы — см. В.3;

- интегрального риска нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации — см. В.4.

В.1.2 Для расчета типовых показателей рисков исследуемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. Под моделируемой системой понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения. Модели и методы прогнозирования рисков в таких системах используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики по процессам и возможным условиям их реализации, а также возможные гипотетичные данные.

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

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

В.1.4 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований по защите информации в системе (в качестве моделируемой системы простой или сложной структуры могут быть рассмотрены выходные результаты с задействованными активами и действия процесса, к которым предъявлены определенные требования по защите информации);

- в условиях неопределенностей возникновение и разрастание различных угроз описывается в терминах случайных событий;

- для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и/или защитных преград, предназначенных для воспрепятствования реализации угроз.

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

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

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

В.1.7 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для мо-

делируемой 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 без учета требований по защите информации, в В.3 приведены способы прогнозирования риска нарушения требований по защите информации в процессе управления инфраструктурой системы (в т. ч. с использованием моделей В.2). Методы прогнозирования интегрального риска нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации представлены в В.4. При этом интегральный риск нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса управления инфраструктурой 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 управления инфраструктурой системы.

В.1.9 Другие возможные подходы к оценке 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 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

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

В.2.1 Общие положения

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

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

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

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

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

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

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

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

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

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

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

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

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, а также в силу иных причин надежность реализации процесса управления инфраструктурой системы может быть нарушена. Такое нарушение способно повлечь за собой негативные последствия.

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

Примечание — С точки зрения надежности реализации процесса примером источников угроз могут служить природные и техногенные угрозы для конкретного оборудования, когда значения отслеживаемого параметра функционирования оборудования (например, температуры, давления) выходят за установленные для него допустимые пределы рабочего или нормативного диапазона значений. Активизация такого источника угроз на практике начинается с момента нарушения допустимого диапазона и завершается реальным отказом или сбоем в работе оборудования, способным привести к ущербу, — см., например, ГОСТ Р 58494.

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

В модели рассмотрен следующий последовательный алгоритм возникновения и развития потенциальной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться. По прошествии времени активизации, свойственного этому источнику угрозы (в общем случае этот время активизации представляет собой случайную величину), наступает виртуальный момент нарушения целостности моделируемой системы, интерпретируемый как момент нарушения надежности реализации рассматриваемого процесса с возможными негативными последствиями. Если после виртуального начала активизации угрозы на временной оси наступает очередная диагностика, 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 мгновенная, это считают эквивалентным внезапному отказу. Усилия системной инженерии как раз и направлены на использование времени постепенной активизации угроз для своевременного выявления, распознавания и противодействия им.

С точки зрения системной инженерии результатом применения модели является расчетная вероятность нарушения надежности реализации процесса управления инфраструктурой системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики) целостности системы.

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

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

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

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

$T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы (без использования метода повышения адекватности модели по В.2.4 действует ограничительное предположение, что среднее время восстановления нарушаемой целостности системы, выявляемой при диагностике, включено в среднее время системной диагностики, т. е. средние времена диагностики без и с восстановлением целостности моделируемой системы приблизительно одинаковы);

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

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

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

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

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

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

Возможны два варианта:

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

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

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

Примечание — Формулу (В.2) используют также для оценки вероятности надежной реализации процесса управления инфраструктурой системы при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по модели В.2.2.

Для варианта 2 при условии независимости исходных характеристик вероятность надежной реализации процесса управления инфраструктурой системы в течение периода прогноза $T_{зад}$ вычисляют по формуле

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

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

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

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

$P_{кон}$ — вероятность надежной реализации процесса управления инфраструктурой системы после последнего системного контроля, вычисляемая по формуле (В.2), т. е.

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

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

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

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

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

В итоге вероятность надежной реализации процесса управления инфраструктурой моделируемой системы, представляемой в виде «черного ящика», в течение периода прогноза $T_{зад}$ определяется аналитическими выражениями (В.2)—(В.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (В.1) вероятность нарушения надежности реализации процесса управления инфраструктурой моде-

лируемой системы $R_{надежн}$ (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 прогнозируемый риск нарушения надежности реализации процесса управления инфраструктурой системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

Примечание — В частном случае, когда период между диагностиками больше периода прогноза $T_{меж} > T_{зад}$, модель В.2.3 превращается в модель В.2.2 для прогноза риска нарушения надежности реализации процесса управления инфраструктурой 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 системы совпадают. В развитие моделей В.2.2 и В.2.3 в настоящем подразделе приведены способы, позволяющие с использованием В.2.2 и В.2.3 создание моделей для систем сложной структуры и более общего случая, когда значения времен системной диагностики и восстановления нарушенных возможностей системы различны.

Расчет основан на применении следующих инженерных способов.

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

2-й способ позволяет переходить от оценок систем или отдельных элементов, представляемых в виде «черного ящика», к оценкам систем неограниченно сложной параллельно-последовательной логической структуры. В формируемой структуре, исходя из реализуемых технологий для системы, состоящей из двух элементов, взаимовлияющих на выполнение процесса, указывается характер их логического соединения. Если два элемента соединяются последовательно, что означает логическое соединение «И», то в контексте надежности реализации процесса это интерпретируется так: «в системе обеспечена 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», 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».

Для комплексной оценки в приложении к сложным системам используются рассчитанные на моделях вероятности нарушения надежности реализации процесса для 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 m-го элемента за заданное время t, $m = 1, 2$.

Рекурсивное применение соотношений (В.6), (В.7) снизу-вверх предоставляет возможности получения соответствующих вероятностных оценок для неограниченно сложной логической структуры с параллельно-последовательным логическим соединением элементов.

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

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.2.2 и В.2.3 и применения 2-го способа получается вероятность нарушения надежности функционирования моделируемой системы 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 функционирования моделируемой системы вплоть до каждого 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 функционирования каждого из элементов и моделируемой системы в целом. С точки зрения системной инженерии в приложении к рассматриваемому процессу, представляемому в виде моделируемой системы простой или сложной структуры, это среднее время может быть интерпретировано как виртуальная средняя наработка на нарушение надежности реализации процесса при прогнозировании риска по моделям В.2.2 и В.2.3. Обратная величина этого среднего времени является частотой нарушений надежности реализации процесса в условиях разнородных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения процесса для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей «черного ящика» В.2.2 и В.2.3. Этот способ используют, когда изначальная статистика для определения частотных характеристик отсутствует или ее недостаточно.

4-й способ в дополнение к возможностям 2-го и 3-го способов позволяет повысить адекватность моделирования за счет развития моделей В.2.2 и В.2.3 в части отдельного учета времени на контроль (диагностику) состояния и восстановление после нарушения целостности моделируемой системы. 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 для восстановления нарушенных возможностей по выполнению процесса на практике требуется дополнительное время ($T_{восст}$), то для моделирования, учитывающего лишь один параметр ($T_{диаг}$) это дополнительное время должно быть также учтено. При этом усредненное время диагностики с учетом дополнительного времени на восстановление вычисляют итеративно с заданной точностью:

- 1-я итерация определяет $T^{(1)}_{диаг} = T_{диаг}$, задаваемое на входе модели В.2.3. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемых возможностей по обеспечению выполнения требований по защите информации;

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

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

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 время 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 та же модель В.2.3.

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

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

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

В.3.1 Общие положения

Прогнозирование рисков нарушения требований по защите информации осуществляют на основе применения математических моделей для прогнозирования риска нарушения требований по защите информации ГОСТ Р 59341—2021 (В.2 приложения В). Все положения по моделированию, изложенные в ГОСТ Р 59341 для процесса управления информацией, в полной мере применимы для прогнозирования риска нарушения требований по защите информации в процессе управления инфраструктурой 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 по-прежнему понимается такое ее состояние, которое в течение задаваемого периода прогноза отвечает целевому назначению системы (см. В.2.1.3). 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 временно́й 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. пребывание в состоянии «Выполнение требований по защите информации в системе нарушено»). В свою очередь вероятность нарушения требований по защите информации в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения требований по защите информации.

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

С формальной точки зрения при сопоставлении с возможным ущербом модель позволяет оценить вероятностное значение риска нарушения требований по защите информации в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения требований по защите информации в процессе управления инфраструктурой 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 — «черного ящика», используют исходные данные, формально определяемые в общем случае следующим образом:

σ — частота возникновения источников угроз нарушения требований по защите информации в процессе управления инфраструктурой 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 нарушений по защите информации в моделируемой системе в течение периода прогноза $T_{зад}$;

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

Расчет показателей применительно к процессу управления инфраструктурой системы для моделируемой системы простой и сложной структуры осуществляют по формулам ГОСТ Р 59341—2021 (В.2 приложения В). Расчет вероятности нарушения требований по защите информации в системе для процесса управления инфраструктурой 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 модели, позволяющие оценивать защищенность от опасных программно-технических воздействий, от несанкционированного доступа и сохранение конфиденциальности информации в системе, — см. ГОСТ Р 59341—2021 (В.2, В.3 приложения В).

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

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

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

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

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

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса управления инфраструктурой системы

Г.1 Анализируемые объекты

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

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

При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможным ущербом. Прогнозирование рисков осуществляют с использованием формализованного представления реальной системы в виде моделируемой системы.

Применительно к конкретной системе в целях прогнозирования рисков согласно 5.3, 6.1 определению подлежат:

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

Г.2 Цель прогнозирования рисков

Основной целью прогнозирования рисков является установление степени вероятного нарушения требований по защите информации и/или нарушения реализации исследуемого процесса управления инфраструктурой 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

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

Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи системного анализа (см. раздел 7). В общем случае моделируемую систему представляют либо в виде «черного ящика» (см. В.2.2 и В.2.3), либо в виде сложной системы, элементы которой логически объединяются последовательно или параллельно (см. В.2.4). Для получения более точных результатов прогнозирования рисков осуществляют декомпозицию сложной моделируемой системы до уровня составных системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых для описания целостности моделируемой системы логическими условиями «И» и «ИЛИ». При этом целостность моделируемой системы (системного элемента) в течение задаваемого периода прогноза означает такое состояние этой системы (системного элемента), которое в течение периода прогноза обеспечивает ее целевое назначение.

Примечания

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

2 Логические условие «ИЛИ» для двух связанных этим условием элементов интерпретируется так: система из двух параллельно соединяемых элементов находится в состоянии целостности, когда первый элемент «ИЛИ» второй элемент находятся в состоянии целостности (в частности, когда для повышения надежности дублируется выполнение отдельных действий).

Для каждого из элементов и для моделируемой системы в целом вводится пространство элементарных состояний (с учетом логических взаимосвязей элементов условиями «И», «ИЛИ»). Например, в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси может быть формально определено двумя основными состояниями (см. также В.3.1):

- «Выполнение требований по защите информации в процессе управления инфраструктурой обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации;

- «Выполнение требований по защите информации в процессе управления инфраструктурой нарушено» — в противном случае, т. е. с точки зрения математического моделирования невыполнение заданных требований считается нарушением целостности элемента.

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

- «Отсутствуют нарушения реализации процесса управления инфраструктурой системы», если в течение всего периода прогноза обеспечено выполнение определенных действий процесса «И» выполнение определенных требований по защите информации;

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

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

В Г.7 приведены примеры прогнозирования рисков.

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

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

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

По мере решения на практике задач анализа и оптимизации применительно к процессу управления инфраструктурой системы создают базы знаний, содержащие варианты решения типовых задач системной инженерии.

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.4 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе, которая может быть представлена в виде «черного ящика» (см. В.2.1, В.2.2, В.3) или сложной логической структуры (см. В.2.3, В.3, В.4), расчетными показателями являются:

$R_{\text{надежн}}(T_{\text{зад}})$ — риск нарушения надежности реализации процесса управления инфраструктурой 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 управления инфраструктурой системы в течение задаваемого периода прогноза $T_{\text{зад}}$;

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

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

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков применительно к процессу управления инфраструктурой системы осуществляют следующие шаги.

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

Шаг 2. Устанавливают конкретные цели прогнозирования. Действия осуществляют согласно Г.2.

Шаг 3. Выявляют перечень существенных угроз, критичных с точки зрения недопустимого потенциального ущерба (см. также ГОСТ Р 59346). 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 согласно рекомендациям Г.4. Выбирают подходящие математические модели и методы повышения их адекватности по В.2, В.3, В.4. Осуществляют расчет выбранных показателей с использованием соотношений (В.1)—(В.10) и иных рекомендаций приложения В.

Г.6 Обработка и использование результатов прогнозирования рисков

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

Г.7 Примеры

Г.7.1 Приводимые примеры демонстрируют отдельные аналитические возможности методических положений, рекомендуемых настоящим стандартом.

Согласно [27] сложившийся уровень развития социально-экономической, транспортной и информационно-коммуникационной инфраструктуры сухопутных территорий Арктической зоны РФ по состоянию на 2020 г. представляет собой множество долговременных разнородных угроз национальной безопасности в Арктике. При освоении Арктики неизбежны неопределенности в специфике решения практических задач, требующих математического моделирования, системного анализа и оптимизации на различных метауровнях.

Учитывая сложность и многогранность решаемых практических задач по освоению Арктики и стремление к эффективной реализации государственной политики РФ в Арктике на период до 2035 года и последующие десятилетия неизбежным является создание единого ЦОД (см. ГОСТ Р 58811, ГОСТ Р 58812), интегрирующего аналитические возможности для решения комплекса задач освоения Арктики. В условиях реальных и потенциальных угроз нарушения безопасности критической информационной инфраструктуры (см. [15]) защита информации в ЦОД имеет приоритетное значение. Не вдаваясь в детали и специфику разнородных инфраструктурных решений, подлежащих интеграции и применению, в рамках примеров продемонстрированы отдельные практические подходы к использованию настоящих методических указаний для решения ряда приоритетных задач освоения Арктики:

- задач развития социально-экономической инфраструктуры (задач 1-го типа), предусматривающих:
- инфраструктурное обустройство минерально-сырьевых центров, логистически связанных с Северным морским путем,
- ускоренное развития социальной инфраструктуры населенных пунктов, в которых расположены органы и организации, выполняющие функции в области обеспечения национальной безопасности и/или функции базы для развития минерально-сырьевых центров, реализации экономических и/или инфраструктурных проектов в Арктике,
- создание эффективной системы предупреждения и ликвидации (минимизации) последствий аварийных разливов нефти и нефтепродуктов на всей протяженности Северного морского пути и других морских транспортных коридоров,
- развитие системы энергоснабжения, модернизации объектов локальной генерации, расширения использования возобновляемых источников энергии, сжиженного природного газа и местного топлива,
- интенсификацию лесовосстановления, стимулирование развития лесной инфраструктуры и глубокой переработки лесных ресурсов;
- задач развития транспортной инфраструктуры (задач 2-го типа), предусматривающих:
- формирование ледокольного, аварийно-спасательного и вспомогательного флотов в составе, необходимом и достаточном для обеспечения круглогодичного, безопасного, бесперебойного и экономически эффективного судоходства в акваториях Северного морского пути и других морских транспортных коридоров,
- строительство и модернизацию морских портов, расширение возможностей судоходства по рекам Арктической зоны, включая проведение дноуглубительных работ, обустройство портов и портопунктов,
- строительство железнодорожных магистралей, обеспечивающих вывоз продукции из регионов европейской и азиатской частей страны по Северному морскому пути,
- расширение сети аэропортов и посадочных площадок, обеспечения транспортной доступности населенных пунктов, не имеющих связи с сетью автомобильных дорог общего пользования;
- задач развития информационно-коммуникационной инфраструктуры (задач 3-го типа), предусматривающих:
- развитие системы и средств постоянного комплексного космического мониторинга Арктики, независимых от иностранных технологий и средств информационного обеспечения,
- создание системы контроля за обеспечением безопасности судоходства, управлением транспортными потоками в районах интенсивного движения судов,
- совершенствование информационно-коммуникационной инфраструктуры, позволяющей оказывать услуги связи населению и хозяйствующим субъектам, в том числе прокладки подводных волоконно-оптических линий связи по трассе Северного морского пути.

В привязке к упомянутым задачам, позволяющей достичь демонстрационные цели примеров, применение методических указаний иллюстрирует прогноз:

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

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

- количественную оценку рисков нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации;
- количественную оценку рисков нарушения требований по защите информации (как поэлементно по каждому типу инфраструктурных задач, так и за весь комплекс задач);
- выявление критичных факторов, влияющих на риски;
- определение такого периода, при котором сохраняются гарантии непревышения допустимых рисков;
- количественную оценку интегрального риска нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации.

Вышеизложенное в Г.7.1 представляет собой пример выполнения шагов 1, 2 настоящих методических указаний (см. Г.5).

Г.7.2 Пример 1 (см. Г.7.3) иллюстрирует прогноз рисков нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации с использованием ЦОД, создаваемого и действующего с учетом рекомендаций ГОСТ Р 58811, ГОСТ Р 58812 и 6.1.3 настоящего стандарта. Пример 2 (см. Г.7.4) иллюстрирует прогноз риска нарушения требований по защите информации непосредственно в ЦОД с ориентацией на инженерную инфраструктуру по ГОСТ Р 58812. Пример 3 (см. Г.7.5) дает представление об интегральном риске нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации.

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

Г.7.3 Пример 1. Моделируемая система примера 1, демонстрирующего прогнозирование риска нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации, представлена на рисунке Г.1. Здесь в качестве моделируемой системы выступает комплекс выходных результатов и активов для решения задач 1-го, 2-го и 3-го типов (см. Г.7.1). Применима следующая интерпретация: в течение задаваемого периода прогноза моделируемая система находится в элементарном состоянии «Целостность моделируемой системы сохранена» (т. е. обеспечена реализация процесса управления инфраструктурой системы, гарантирующая надежное получение выходных результатов), если каждый из элементов в течение всего периода находится в состоянии «Целостность элемента моделируемой системы сохранена» (т. е. обеспечена надежная реализация процесса управления инфраструктурой системы для решения задач развития социально-экономической, транспортной «И» информационно-коммуникационной инфраструктуры).

При выполнении шага 3 настоящих методических указаний (см. Г.5) выявлено множество возможных угроз, влияющих на надежность получения выходных результатов по каждому из структурных элементов. Не углубляясь в многочисленные технические аспекты постановки и решения задач развития социально-экономической, транспортной и информационно-коммуникационной инфраструктуры в Арктике (т. е. всех трех элементов, представленных на рисунке Г.1), в таблице Г.1 отражены гипотетичные усредненные исходные данные с возможным обоснованием принятых значений для моделирования по моделям В.2.2 и В.2.3 настоящего стандарта.

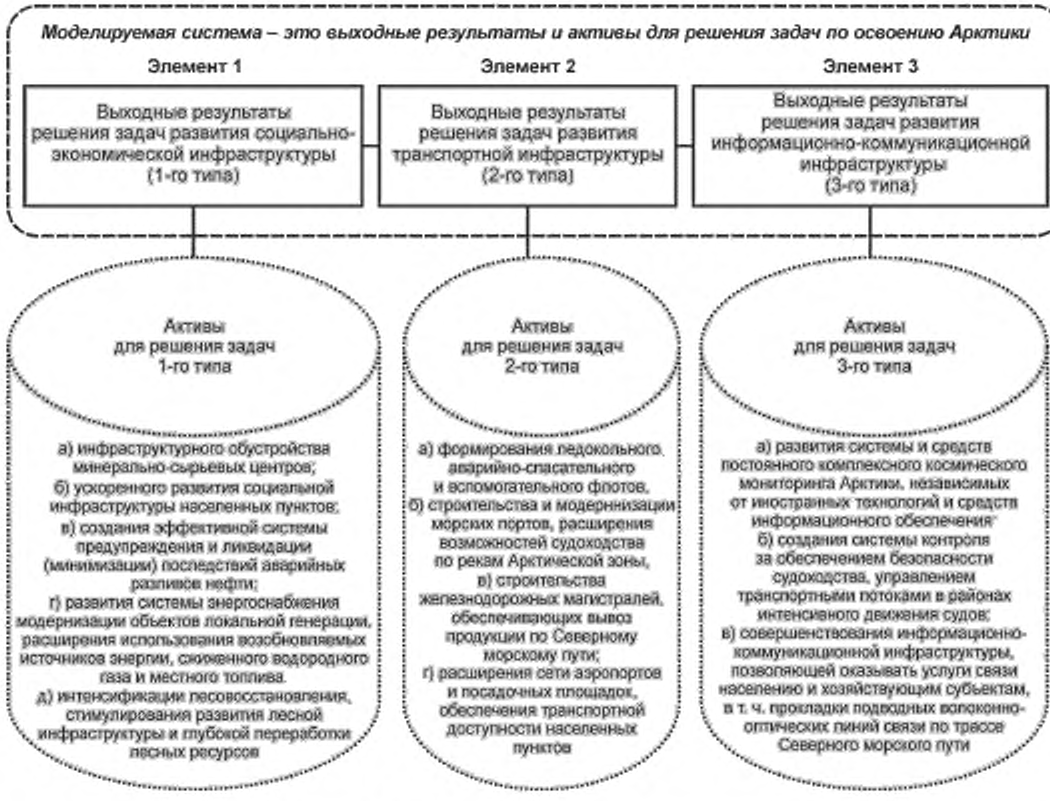


Рисунок Г.1 — Моделируемая система для примера 1

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

Исходные данные	Значения и комментарии		
	для 1-го элемента, т. е. для решения задач развития социально-экономической инфраструктуры	для 2-го элемента, т. е. для решения задач развития транспортной инфраструктуры	для 3-го элемента, т. е. для решения задач развития информационно-коммуникационной инфраструктуры
σ — частота возникновения источников угроз нарушения надежности реализации процесса для элемента	2 раза в год (из-за проблем, связанных с трудностями доставки грузов в условиях Арктики и недостатка квалифицированных кадров)	1 раз в год (из-за проблем, связанных с технической и технологической сложностью решаемых задач и недостатка квалифицированных кадров)	1 раз в месяц (из-за проблем, связанных с отставанием в области ИТ, приобретением и использованием несертифицированного импортного ПО, не сертифицированного по требованиям безопасности, и несовершенного отечественного ПО для информационно-коммуникационной инфраструктуры)

Окончание таблицы Г.1

Исходные данные	Значения и комментарии		
	для 1-го элемента, т. е. для решения задач развития социально-экономической инфраструктуры	для 2-го элемента, т. е. для решения задач развития транспортной инфраструктуры	для 3-го элемента, т. е. для решения задач развития информационно-коммуникационной инфраструктуры
β — среднее время развития угроз для элемента с момента возникновения источников угроз до нарушения с возможным ущербом	6 мес (что соизмеримо со временем между критичными проблемами, выявляемыми на практике эксплуатации социально-экономической инфраструктуры) — это означает, что развитие угроз до возможного недопустимого ущерба из-за трудностей в доставке грузов и недостатка квалифицированных кадров составляет в среднем около 6 мес. В течение этого срока за счет управленческих воздействий возможно предотвращение ущерба	2 мес (что соизмеримо со временем между критичными проблемами, выявляемыми при испытаниях или эксплуатации объектов создаваемой транспортной инфраструктуры) — это означает, что развитие угроз до возможного недопустимого ущерба из-за технической и технологической сложности решаемых задач и недостатка квалифицированных кадров составляет в среднем около 2 мес. В течение этого срока за счет контроля и соответствующих управленческих воздействий возможно предотвращение ущерба	2 нед (что соизмеримо со временем между критичными ошибками в ПО, выявляемыми в процессе функционирования и при развитии информационно-коммуникационной инфраструктуры) — это означает, что развитие угроз до возможного недопустимого ущерба из-за отставания в области ИТ, приобретения и использования несертифицированного импортного ПО, не сертифицированного по требованиям безопасности, и несовершенного отечественного ПО составляет в среднем около 3 мес. В течение этого срока за счет контроля и соответствующих управленческих воздействий возможно предотвращение ущерба
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей элемента	1 нед/по результатам системного анализа снижается до суток — определяется регламентом текущего контроля решения социально-экономических задач со стороны руководства поселений и предприятий	1 нед/по результатам системного анализа снижается до суток — определяется регламентом текущего контроля решения задач развития транспортной инфраструктуры со стороны руководства предприятий	1 ч — определяется регламентом автоматического контроля технологической безопасности используемой информационно-коммуникационной инфраструктуры
$T_{диаг}$ — среднее время диагностики состояния элемента	1 ч — определяется временем удаленного сеанса связи для текущего контроля состояния решения социально-экономических задач	1 ч — определяется временем удаленного сеанса связи для текущего контроля состояния решения задач развития транспортной инфраструктуры	1 мин — автоматический контроль технологической безопасности используемой информационно-коммуникационной инфраструктуры
$T_{восст}$ — среднее время восстановления элемента после выявления нарушений	3 дня — это время экстренного устранения на местах негативных последствий от неадекватного решения проблем, приведших к недопустимым ущербам	1 нед — это время экстренного устранения на местах негативных последствий от неадекватного решения проблем, приведших к недопустимым ущербам	30 мин — это среднее время восстановления работоспособности информационно-коммуникационной инфраструктуры (возможно, за счет перевода в дежурный технологический режим функционирования) после критичных нарушений, приведших к недопустимым ущербам
$T_{зад}$ — задаваемая длительность периода прогноза	от 1 года до 4 лет работы по освоению Арктики (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения надежности реализации процесса управления инфраструктурой системы)		

При выполнении шагов 4 и 5 настоящих методических указаний (см. Г.5) прогнозирование риска нарушения надежности реализации процесса управления инфраструктурой 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. Для расчетов в качестве точечного периода прогноза выбран срок 2 года, который характерен для кратко- и среднесрочных планов реального создания и развития многих инфраструктурных проектов при освоении Арктики.

Анализ результатов расчетов показал, что в вероятностном выражении риск нарушения надежности реализации процесса без учета требований по защите информации в течение двух лет составит за все элементы 0,282, в т. ч. по 1-му элементу 0,089, по 2-му — 0,182, а по 3-му — 0,036 (см. рисунок Г.2). В свою очередь для прогноза на 1 год вероятность нарушения надежности реализации процесса без учета требований по защите информации не опустится ниже 0,150 (см. рисунок Г.3), а для прогноза на 4 года при еженедельном контроле вероятности нарушения надежности и успешной реализации процесса практически сравняются (0,49 против 0,51). На практике такой уровень рисков неприемлем, т. е. необходим поиск критичных факторов, влияющих на риски, и обоснование действенных способов снижения рисков.

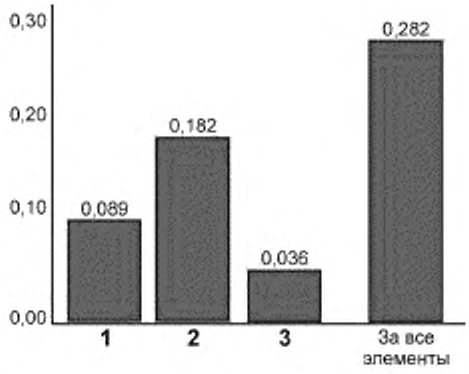


Рисунок Г.2 — Риски нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации по элементам 1—3 и за все элементы в течение 2 лет при еженедельном контроле

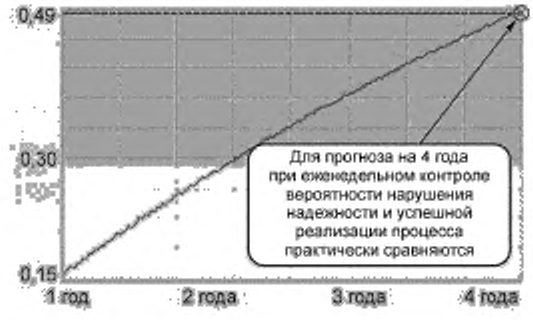


Рисунок Г.3 — Зависимость риска нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации по всем элементам от длительности периода прогноза (от 1 до 4 лет) при еженедельном контроле

Дополнительные расчеты показали, что одним из критичных факторов выступает параметр «среднее время между окончанием предыдущей и началом очередной диагностики возможностей» для 1-го и 2-го элементов ($T_{меж}$). За счет управленческого решения, выражающегося в изменении частоты контроля с еженедельного до ежесуточного, с принятием соответствующих мер противодействия угрозам при прочих неизменных условиях возможно снижение рисков в несколько раз. Достаточно сравнить риски на рисунках Г.2 и Г.4: по всем элементам достигнуто снижение риска в 2,1 раза, по 1-му элементу — в 4 раза, по 2-му элементу — в 1,7 раза, по 3-му элементу — в 2,6 раза. То есть за счет наиболее просто осуществляемых организационных мер, связанных с введением более частого контроля работ по развитию социально-экономической и транспортной инфраструктуры, достижимо существенное снижение рисков нарушения надежности реализации процесса управления инфраструктурой системы. Возможность достижения такого неочевидного эффекта выявлена на основе применения расчетных моделей В.2.2, В.2.3. Для прогноза на 1 год вероятность нарушения надежности реализации процесса без учета требований по защите информации составит 0,08 (см. рисунок Г.5). В свою очередь, в результате анализа расчетной зависимости риска от длительности периода прогноза (от 1 до 4 лет) дополнительно установлено, что в условиях примера при ежесуточном контроле уровень риска 0,10 не будет превышен в течение 1,3 года. Это означает, что, ориентируясь для процесса управления инфраструктурой при освоении Арктики на задаваемый допустимый риск на уровне 0,10, в условиях примера в течение 1,3 года будут сохранены гарантии непревышения допустимого риска.

Примечание — Слабозаметный пилообразный характер зависимости риска от периода прогноза на рисунках Г.3, Г.5 объясняется периодичностью диагностик с восстановлением целостности моделируемой системы и тем, что в моделях В.2.2, В.2.3 при расчетах используется целое количество диагностик, входящих в период прогноза. Сразу после диагностики риск нарушения снижается, со временем до следующей диагностики возрастает. Именно это является причиной некоторой пилообразности.

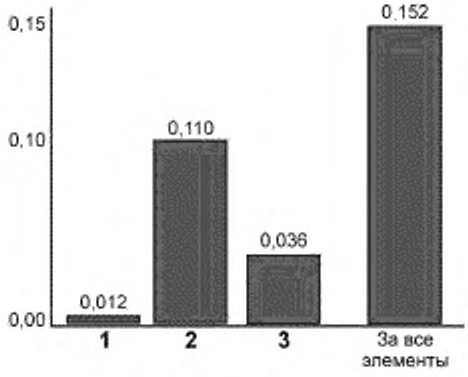


Рисунок Г.4 — Риски нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации по элементам 1—3 и за все элементы в течение 2 лет при ежесуточном контроле

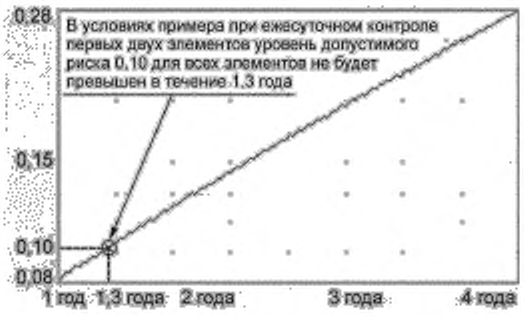


Рисунок Г.5 — Зависимость риска нарушения надежности реализации процесса управления инфраструктурой системы без учета требований по защите информации по всем элементам от длительности периода прогноза (от 1 до 4 лет) при ежесуточном контроле

Г.7.4 Пример 2. Моделируемая система примера 2, демонстрирующего прогнозирование риска нарушения требований по защите информации, представлена на рисунке Г.6. В отличие от примера 1 моделируемая система представляет собой комплекс действий, связанных с:

- обслуживанием зданий и сооружений (элемент 1);
- обеспечением функционирования инженерно-технических систем (элемент 2);
- обеспечением функционирования инженерных сетей (элемент 3);
- решением задач развития социально-экономической инфраструктуры (элемент 4);
- решением задач развития транспортной инфраструктуры (элемент 5);
- решением задач развития информационно-коммуникационной инфраструктуры (элемент 6).

Применима следующая интерпретация: в течение задаваемого периода прогноза моделируемая система находится в элементарном состоянии «Выполнение требований по защите информации в системе обеспечено», если все учитываемые элементы в течение всего периода находятся в состоянии «Выполнение требований по защите информации для элемента обеспечено».

Не вдаваясь в детали осуществляемых действий на уровне инженерной инфраструктуры и функциональной части ЦОД, в таблице Г.2 отражены гипотетичные усредненные исходные данные с возможным обоснованием принятых значений для расчетов по моделям В.3 настоящего стандарта.

При выполнении шага 4 методики (см. Г.5) прогнозирование риска нарушения требований по защите информации осуществлено с использованием рекомендаций В.3. Для сохранения преемственности с примером 1 в качестве точечного периода прогноза по-прежнему выбран срок 2 года, характерный для кратко- и среднесрочных планов реального создания и развития многих инфраструктурных проектов при освоении Арктики.

Анализ результатов расчетов показал, что в вероятностном выражении риск нарушения требований по защите информации в течение двух лет составит за все элементы 0,219, в т. ч. по 1-му элементу — 0,122, по 2-му — 0,063, по 3-му — 0,032, по элементам 4, 5 и 6 — не превысит 0,011 (см. рисунок Г.7). В свою очередь, для прогноза на 4 года при ежесуточном контроле состояния инженерной инфраструктуры ЦОД (т. е. элементов 1, 2, 3) вероятность нарушения требований по защите информации за все действия ЦОД (т. е. элементы 1—6) составит около 0,39, а для прогноза на 1 год эта вероятность составит около 0,12 (см. рисунок Г.8). В целом результаты соизмеримы с результатами примера 1.

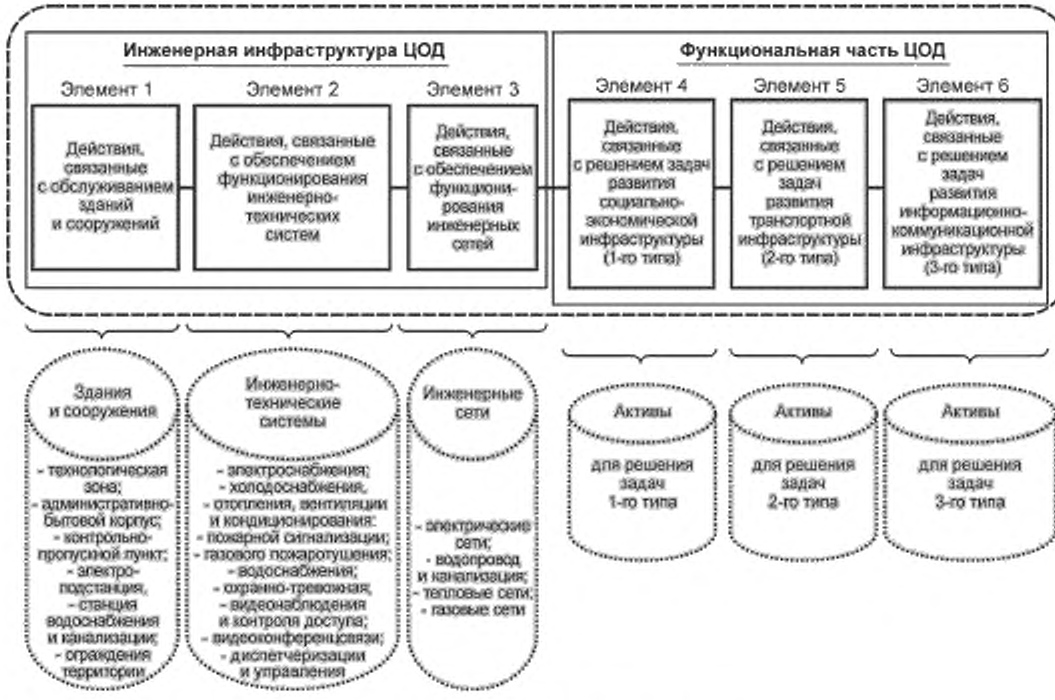


Рисунок Г.6 — Моделируемая система для примера 2

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

Исходные данные	Элементы	Значения и комментарии
σ — частота возникновения источников угроз нарушения требований по защите информации	Элемент 1	4 раза в год, что соизмеримо с возникновением угроз, связанных с субъективными факторами и ошибками специалистов средней квалификации в области ИТ при решении задач обслуживания зданий и сооружений
	Элемент 2	2 раза в год, что соизмеримо со временем наработки на отказ инженерно-технического оборудования при его функционировании
	Элемент 3	1 раз в год, что соизмеримо с возникновением угроз, связанных с причинами человеческих ошибок в обслуживании инженерных сетей
	Элемент 4	1 раз в 2 год, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения при решении задач развития социально-экономической инфраструктуры
	Элемент 5	1 раз в 2 год, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения при решении задач развития транспортной инфраструктуры
	Элемент 6	2 раза в год, что соизмеримо с возникновением угроз от использования импортного технического и программного обеспечения при обеспечении функционирования и решении задач развития информационно-коммуникационной инфраструктуры

Окончание таблицы Г.2

Исходные данные	Элементы	Значения и комментарии
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	По всем элементам 1—6	1 мес (предполагается, что в целях скрытности источники угроз активизируются не сразу, а с некоторой задержкой не менее месяца) — это время до возможного ущерба после возникновения признаков возможных угроз
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	Элемент 1	24 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при сменной работе по обслуживанию зданий и сооружений
	Элемент 2	24 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при сменной работе по обслуживанию инженерно-технического оборудования
	Элемент 3	24 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при сменной работе по обслуживанию инженерных сетей
	Элемент 4	8 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при решении задач развития социально-экономической инфраструктуры
	Элемент 5	8 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при решении задач развития транспортной инфраструктуры
	Элемент 6	1 ч — определяется регламентом контроля целостности программного обеспечения и активов ЦОД при обеспечении функционирования и решении задач развития информационно-коммуникационной инфраструктуры
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы	По всем элементам 1—6	30 с, что соизмеримо с длительностью автоматического контроля целостности программного обеспечения и активов ЦОД
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	По всем элементам 1—6	10 мин, включая перезагрузку программного обеспечения и восстановление данных ЦОД
$T_{зад}$ — задаваемая длительность периода прогноза	По всем элементам 1—6	От 1 года до 4 лет работ по освоению Арктики (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения требований по защите информации)



Рисунок Г.7 — Риски нарушения требований по защите информации по элементам 1—6 и за все элементы в течение 2 лет при ежесуточном контроле состояния объектов инженерной инфраструктуры ЦОД

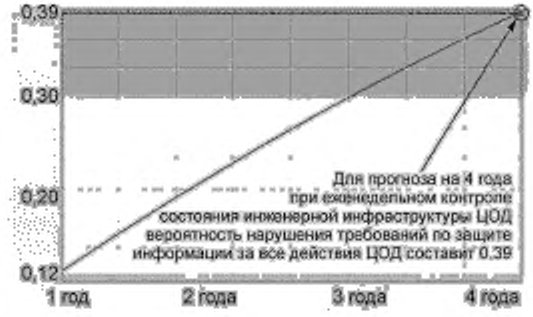


Рисунок Г.8 — Зависимость риска нарушения требований по защите информации по всем элементам ЦОД от длительности периода прогноза (от 1 до 4 лет) при ежесуточном контроле состояния объектов инженерной инфраструктуры ЦОД

По аналогии с примером 1 одним из критичных факторов выступает параметр $T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей для инженерной инфраструктуры ЦОД (т. е. для 1-го, 2-го и 3-го элементов). За счет управленческого решения, выражающегося в изменении частоты контроля с ежесуточного до одного раза в 8 ч (что можно связать со сменной работой на объектах), с принятием соответствующих мер противодействия угрозам при прочих неизменных условиях возможно снижение рисков за все действия ЦОД (т. е. по всем элементам 1—6) с уровня 0,219 до 0,091 (сравните риски на рисунках Г.7 и Г.9). Таким образом, за счет наиболее просто осуществляемых организационных мер, связанных с введением более частого контроля состояния инженерной инфраструктуры (например, силами дежурной службы обеспечения информационной безопасности ЦОД), достижимо существенное снижение рисков нарушения требований по защите информации. Такой эффект выявлен на основе применения моделей и рекомендаций В.3. Для прогноза на 1 год вероятность нарушения требований по защите информации составит 0,05 (см. рисунок Г.10). В результате анализа расчетной зависимости риска от длительности периода прогноза (от 1 до 4 лет) дополнительно установлено, что в условиях примера при контроле инженерной инфраструктуры 1 раз в 8 ч уровень риска 0,10 не будет превышен в течение 2,3 года. Это означает, что, ориентируясь для процесса управления инфраструктурой при освоении Арктики на задаваемый допустимый риск нарушения требований по защите информации на уровне 0,10, в течение 2,3 года будут сохранены гарантии непревышения допустимого риска для условий таблицы Г.1. Это в 1,77 раза дольше по сравнению с аналогичным гарантийным сроком из примера 1.



Рисунок Г.9 — Риски нарушения требований по защите информации по элементам 1—6 и за все элементы в течение 2 лет при контроле состояния объектов инженерной инфраструктуры ЦОД каждые 8 ч

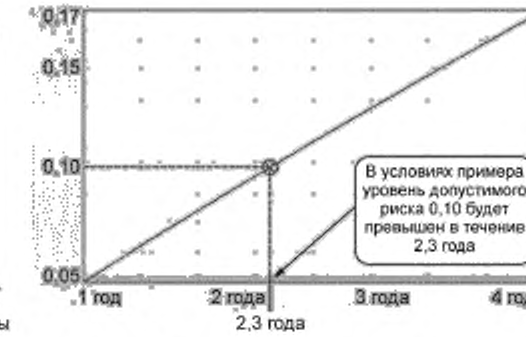


Рисунок Г.10 — Зависимость риска нарушения требований по защите информации по всем элементам ЦОД от длительности периода прогноза (от 1 до 4 лет) при контроле состояния объектов инженерной инфраструктуры ЦОД каждые 8 ч

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

По результатам 1-го примера $R_{надежн}(T_{зад}) = 0,08$ (см. рисунок Г.5), а по результатам 2-го примера $R_{наруш}(T_{зад}) = 0,05$ (см. рисунок Г.10). Тогда по формуле (В.10)

$$R_{интегр}(T_{зад}) = 1 - (1 - 0,08)\cdot(1 - 0,05) \approx 0,126.$$

В итоге интегральный риск нарушения реализации процесса управления инфраструктурой системы в течение года с учетом требований по защите информации составит 0,126. В общем случае такой уровень риска считается повышенным, он может быть признан приемлемым лишь в исключительных случаях, когда отсутствуют реальные возможности какого-либо противодействия угрозам. Поскольку такие возможности далеко не исчерпаны, необходим дополнительный поиск мер для снижения интегрального риска.

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

Примечание — Другие примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Г.8 Материально-техническое обеспечение

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

Г.9 Отчетность

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

Приложение Д
(справочное)

Типовые допустимые значения показателей рисков для процесса управления инфраструктурой системы

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

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

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

Типовые допустимые значения количественных показателей рисков для процесса управления инфраструктурой 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 реализации рассматриваемого процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Пример задания допустимых значений рисков

Показатель	Допустимое значение риска (в вероятностном выражении)	
	при ориентации на обоснование по прецедентному принципу	при ориентации на обоснование для системы-эталона
Риск нарушения требований по защите информации в процессе управления инфраструктурой системы	Не выше 0,10	Не выше 0,05
Интегральный риск нарушения реализации процесса управления инфраструктурой системы с учетом требований по защите информации	Не выше 0,10	Не выше 0,05

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса управления инфраструктурой системы

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

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

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

Е.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления инфраструктурой 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 управления инфраструктурой.

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). (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)

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

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

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

Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 30.04.2021. Подписано в печать 24.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5.12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru