ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59349— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ СИСТЕМНОГО АНАЛИЗА

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 18 мая 2021 г. № 372-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 системного анализа . . . 7
5 Общие требования системной инженерии по защите информации в процессе системного анализа . . . 9
6 Специальные требования к количественным показателям . . . 10
7 Требования к системному анализу . . . 13
Приложение А (справочное) Пример перечня защищаемых активов . . . 17
Приложение Б (справочное) Пример перечня угроз . . . 18
Приложение В (справочное) Типовые модели и методы прогнозирования рисков . . . 19
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса системного анализа . . . 31
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса системного анализа . . . 66
Приложение Е (справочное) Примерный перечень методик системного анализа . . . 68
Библиография . . . 69

Введение

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

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

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

- для процессов технического управления — процессов планирования, 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, архитектуры, проекта, 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 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357. Для процесса системного анализа — по настоящему стандарту.

Стандарт устанавливает основные требования системной инженерии по защите информации в процессе системного анализа и специальные требования к используемым количественным показателям.

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 СИСТЕМНОГО АНАЛИЗА

System engineering. Protection of information in system analysis process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения по защите информации в процессе системного анализа, применимого в различных областях системной инженерии.

В приложениях А—Е приведены примеры перечней активов, подлежащих защите, и угроз, типовые модели, методы и методические указания по прогнозированию рисков для процесса системного анализа, 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 системного анализа, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем (см. примеры систем в [1] — [28]).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ 27.003 Надежность в технике. Состав и общие правила задания требований по надежности

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

Издание официальное

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

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

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

ГОСТ 33981 Оценка соответствия. Исследование проекта продукции

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 58045 Авиационная техника. Менеджмент риска при обеспечении качества на стадиях жизненного цикла. Методы оценки и критерии приемлемости риска

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

ГОСТ Р 59337—2021 Системная инженерия. Защита информации в процессе оценки и контроля проекта

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р МЭК 61508-5 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

ГОСТ Р МЭК 62508 Менеджмент риска. Анализ влияния на надежность человеческого фактора

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

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 27.003, ГОСТ 34.003, ГОСТ Р 27.403, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 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 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 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.2

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.3

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.5

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

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

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

3.1.8 **надежность реализации процесса системного анализа:** Свойство процесса системного анализа сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить его в заданных условиях реализации.

3.1.9

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.10

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.11 **принятие решения в режиме реального времени:** Принятие решения в сложившихся условиях за такое время, в течение которого выполнение предупреждающих действий является практически осуществимым и обоснованно целесообразным.

3.1.12

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.13 **система-эталон:** Реальная или гипотетичная система, которая по своим показателям интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации принимается в качестве эталона для полного удовлетворения требований заинтересованных сторон системы и рационального решения задач системного анализа, связанных с обоснованием допустимых рисков, обеспечением нормы эффективности защиты информации, обоснованием мер, направленных на достижение целей процесса, противодействие угрозам и определение сбалансиро-

ванных решений при средне- и долгосрочном планировании, а также с обоснованием предложений по совершенствованию и развитию системы защиты информации.

3.1.14

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.1.15 **скрытая угроза системе:** Угроза системе, выявление которой осуществляется по признакам, косвенно связанным с явными угрозами системе, а распознавание — путем оценки развития предпосылок к нанесению ущерба системе.

3.1.16

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]

3.1.17 **угроза системе:** Совокупность условий и/или факторов, создающих потенциально или реально существующую опасность, связанную с нанесением ущерба системе.

3.1.18

ущерб: Отрицательные последствия, возникающие вследствие причинения вреда активам.

[ГОСТ Р 53113.1—2008, пункт 3.38]

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

3.1.20

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.1.21 **явная угроза системе:** Угроза системе, выявление и распознавание которой однозначно возможно по заранее определенным и реально проявляемым признакам.

3.2 В настоящем стандарте использованы следующие сокращения:

СУР — система управления рисками;

ТЗ — техническое задание;

ТЭК — топливно-энергетический комплекс;

УВМП — универсальная вспомогательная модель показателя.

4 Основные положения системной инженерии по защите информации в процессе системного анализа

4.1 Общие положения

Организации используют процесс системного анализа для прогнозирования рисков и обоснования допустимых рисков, выявления явных и скрытых угроз системе и поддержки принятия решений в жизненном цикле при создании (модернизации, развитии) и эксплуатации системы, а также при выведении системы из эксплуатации.

В процессе системного анализа 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.

Определение выходных результатов процесса системного анализа и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839.

Количественную оценку рисков, свойственных процессу, осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ 59356, ГОСТ Р 59357.

4.2 Стадии и этапы жизненного цикла системы

Процесс системного анализа может быть использован на любой стадии жизненного цикла системы.

Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации систем 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 27.403, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 53622, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58045. Процесс системного анализа может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.3 Цели процесса и назначение мер защиты информации

4.3.1 Определение целей процесса системного анализа осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508 с учетом специфики системы.

В общем случае главной целью процесса системного анализа является удовлетворение аналитических потребностей заинтересованных сторон в поддержке принятия актуальных решений в течение жизненного цикла системы относительно понимания ее функциональных возможностей, результативности, контроля состояния эксплуатационной среды, прогнозирования и определения допустимых рисков, выявления явных и скрытых угроз, оценки и обоснования стратегий, технического облика и сбалансированных системных решений и планов, сравнения альтернатив, выработки критериев и осуществления прогноза безопасности, качества и эффективности системы для задаваемых условий, выработки требований к характеристикам и показателям функционирования системы, оценки свойств и критичности влияния различных параметров на поведение системы, рациональной настройки параметров, разрешения противоречий и поддержания устойчивости функционирования системы.

4.3.2 Меры защиты информации в процессе системного анализа предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [21] — [24] с учетом специфики системы и реализуемой стадии ее жизненного цикла.

4.4 Основные принципы

При планировании и реализации процесса системного анализа руководствуются следующими основными принципами:

- принципом системности, предполагающим наличие целеполагания при реализации процессов, необходимость декомпозиции системы, выполняемых процессов и составных действий, которые могут подвергаться разнородным угрозам безопасности информации;
- принципом целостности, предполагающим связанность выполняемых действий для достижения целей системы и реализуемых для этого процессов;
- принципом системного контроля выполнения требований по защите информации применительно к активам, информация которых или о которых подлежит защите;
- принципом унификации и стандартизации системных решений при планировании и реализации процесса;

- принципом ориентации на обеспечение приемлемого качества, безопасности и эффективности системы, а также эффективности защиты информации в условиях создания (модернизации, развитии), эксплуатации системы и выведения ее из эксплуатации;
- принципом эффективного управления рисками;
- принципом дифференциации требований по защите информации в зависимости от категории значимости системы, проектов и значимости оперируемой информации (см. ГОСТ Р 59346);
- прецедентным принципом для обоснования допустимых рисков в случае его предпочтительности в сравнении с ориентацией на систему-эталон (см. 7.3.3 и приложение Д).

Все основные принципы включают в себя принцип целенаправленности осуществляемых действий в планируемых и реализуемых процессах на протяжении всего жизненного цикла системы.

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе системного анализа 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 потенциально существенных 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 самого процесса.

5 Общие требования системной инженерии по защите информации в процессе системного анализа

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию, развитие системы или на работы по выведению системы из эксплуатации. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы, в качестве которой может выступать система защиты информации, в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований по защите информации формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например, [1] — [28]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов (см. ГОСТ Р 59346).

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

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

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

Требования системной инженерии по защите информации в процессе системного анализа включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе системного анализа определяют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58045 с учетом тре-

бований нормативно-правовых документов, специфики системы и реализуемой стадии ее жизненного цикла (см., например, [1] — [28]).

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

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциально существенных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57839, ГОСТ Р 58045, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, [21] — [24].

Примеры перечней учитываемых активов и угроз в процессе системного анализа приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процесса системного анализа оценивают по показателям рисков в зависимости от специфики системы, целей ее применения и возможных угроз при выполнении процесса. Используют модель угроз безопасности информации.

Системный анализ осуществляют с использованием методов, моделей и методик (см. приложения В, Г, Д, Е) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58045, 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, ГОСТ Р МЭК 62508.

5.7 Для обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах применяют системный анализ с использованием устанавливаемых специальных качественных и количественных показателей рисков. Качественные показатели для оценки рисков в области информационной безопасности определены в ГОСТ Р ИСО/МЭК 27005. Целесообразность использования количественных показателей рисков в дополнение к качественным показателям может потребовать дополнительного обоснования. Состав специальных количественных показателей рисков для системного анализа определен в 6.3.

Типовые модели и методы процесса системного анализа, 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 защиты информации и действий по защите информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам и возможным условиям их реализации.

6 Специальные требования к количественным показателям

6.1 Общие положения

6.1.1 В отношении защищаемых активов, действий и выходных результатов процесса системного анализа, 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 системного анализа являются:

- направления и проблематика необходимых исследований системы;
- принятые критерии, согласованные условия, предположения и принятые допущения при проведении системного анализа, логические правила интерпретации результатов системного анализа;
- требования к обеспечивающим системам или системным элементам, необходимые для осуществления действий системного анализа;
- доступ к обеспечивающим системам или услугам, необходимым для системного анализа;
- модели, методы и методики системного анализа, обоснования их адекватности;
- задокументированные результаты системного анализа, представляемые для принятия решений заинтересованным сторонам.

6.1.3 Для получения выходных результатов процесса системного анализа в общем случае выполняют следующие основные действия:

- подготовку к проведению системного анализа, включая:
  - определение проблем и/или вопросов, требующих системного анализа, и сторон, заинтересованных в проведении системного анализа;
  - формулирование целей системного анализа, установление их связи с удовлетворением аналитических потребностей заинтересованных сторон в поддержке принятия решений в жизненном цикле системы;
  - определение области исследований, обоснование условий, предположений и допущений для обеспечения адекватности проводимого системного анализа;
  - определение и согласование стратегии системного анализа, в т. ч. установление критериев и логических правил интерпретации получаемых результатов;
  - выбор из существующих или разработку специальных методов, моделей и методик, применимых для системного анализа;
  - определение и планирование действий, в т. ч. относительно необходимых обеспечивающих систем или услуг, которые предназначены для поддержки системного анализа, получение или приобретение доступа к ним;
  - сбор исходных данных, их систематизацию и подготовку в виде, пригодном для применения методов, моделей и методик системного анализа;
- непосредственно проведение системного анализа, включая:
  - применение выбранных или специально разработанных методов, моделей и методик системного анализа для разрешения выявленных проблем и вопросов, в т. ч. относительно понимания функциональных возможностей системы, результативности, контроля состояния эксплуатационной среды, прогнозирования и определения допустимых рисков, выявления явных и скрытых угроз, оценки и обоснования стратегий, технического облика и сбалансированных системных решений и планов, сравнения альтернатив, выработки критериев и осуществления прогноза безопасности, качества и эффективности системы для задаваемых условий, выработки требований к характеристикам и показателям функционирования системы, оценки свойств и критичности влияния различных параметров на поведение системы, рациональной настройки параметров, разрешения противоречий и поддержания устойчивости функционирования системы;
  - анализ получаемых результатов системного анализа на предмет их непротиворечивости и согласованности;
  - логическую интерпретацию получаемых результатов и их рассмотрение с точки зрения решения задач системной инженерии и поддержки принятия решений в жизненном цикле системы;
  - формулирование выводов, заключений и рекомендаций по результатам системного анализа;
  - документирование результатов системного анализа, доведение их до всех заинтересованных сторон для принятия решений;
- управление системным анализом, включая:
  - поддержку двунаправленной прослеживаемости между результатами системного анализа и анализируемыми сущностями системы, что должно обеспечивать прослеживание логики в обоснованиях и/или принимаемых решениях;
  - сопровождение результатов системного анализа в жизненном цикле системы для рационального решения актуальных задач системной инженерии.

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

Эффективность защиты информации оценивают с использованием количественных показателей, которые позволяют сформировать представление о текущих и потенциальных проблемах или о возможных причинах недопустимого снижения эффективности на ранних этапах проявления явных и скрытых угроз безопасности информации, когда можно принять предупреждающие корректирующие действия. Дополнительно могут быть использованы вспомогательные статистические показатели, характеризующие события, которые уже произошли, и их влияние на эффективность защиты информации при реализации процесса. Вспомогательные показатели позволяют исследовать произошедшие события и их последствия и сравнивать эффективность применяемых и/или возможных мер в действующей системе защиты информации.

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе системного анализа используют следующие количественные показатели.

- риск нарушения надежности реализации рассматриваемых процессов без учета требований по защите информации (применительно к системным процессам соглашения, процессам организационного обеспечения проекта, процессам технического управления, техническим процессам) — см. В.3, В.4;
- риск нарушения требований по защите информации в процессе системного анализа — см. В.5;
- интегральный риск нарушения надежности реализации процесса системного анализа с учетом требований по защите информации — см. В.6.

6.3.2 Риск нарушения надежности реализации рассматриваемых процессов без учета требований по защите информации характеризуют соответствующей вероятностью в зависимости от учитываемых факторов (без учета требований по защите информации) в сопоставлении с возможным ущербом.

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

6.3.4 Интегральный риск нарушения надежности реализации процесса системного анализа 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 в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

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

7.1 Общие положения

7.1.1 Настоящие требования применимы не только непосредственно к процессу системного анализа, но и к другим стандартизованным процессам в жизненном цикле систем согласно ГОСТ Р 57193, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357. Требования ориентированы на обеспечение защиты информации с точки зрения решения задач системной инженерии.

Настоящие требования к системному анализу процессов в жизненном цикле систем включают в себя:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в жизненном цикле создаваемой (модернизируемой) системы или системы, выводимой из эксплуатации.

Примечание — В общем случае выполнение этих требований способствует достижению целей процесса системного анализа.

7.1.2 При обосновании и формулировании требований к системному анализу руководствуются положениями 7.2—7.5 с учетом специфики системы и рекомендаций ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ 33981, ГОСТ IEC 61508-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58045, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7.

7.2 Требования к прогнозированию рисков

7.2.1 Для прогнозирования рисков в рассматриваемом процессе должны быть:

- определены перечни выходных результатов и составных действий процесса, а для каждого из них — используемые активы (см. приложение А) и потенциально существенные угрозы безопасности информации (см. приложение Б);
- определены количественные показатели прогнозируемых рисков, выбраны, адаптированы или разработаны модели и методики для прогнозирования рисков (см. приложения В, Г, Д, Е);
- реализованы сбор и обработка исходных данных, обеспечивающих применение моделей и методик для прогнозирования рисков;
- предусмотрен механизм использования результатов прогнозирования рисков.

7.2.2 Прогнозирование рисков используют для формального решения задач, связанных с ранним распознаванием и оценкой развития предпосылок к нарушению требований по защите информации, обоснованием эффективных предупреждающих мер по снижению рисков или их удержанием в допустимых пределах, выявлением явных и скрытых угроз, поддержкой принятия решений по выполнению процессов и обеспечению выполнения норм эффективности защиты информации. В зависимости от целей решаемых задач прогнозируемый риск связывают с заранее определенным периодом прогноза (например, на месяц, год, на несколько лет), с моделями угроз, ожидаемых для этого периода.

7.3 Требования к обоснованию допустимых рисков

7.3.1 Допустимые риски нарушения требований по защите информации в рассматриваемом процессе выступают в качестве количественных норм эффективности защиты информации.

Допустимые риски определяют при планировании и реализации процесса и задают во внутренних документах организации. Допустимые риски могут быть установлены в договорах, соглашениях и ТЗ в качественной и/или количественной форме с учетом специфики системы.

7.3.2 Количественное обоснование допустимых рисков осуществляют по прецедентному принципу или с использованием ориентации на риски, свойственные системе-эталону, которая выбирается в качестве аналога для рассматриваемой системы (см. приложение Д).

7.3.3 В результате моделирования различных произошедших событий формируют базу знаний, устанавливающую соответствие расчетных значений прогнозируемых рисков тем реальным событиям, которые состоялись и оказались свойственными этим ситуациям. Соответствие устанавливают по журналам регистрации нарушений требований по защите информации, регистрации случаев нарушения надежности реализации рассматриваемого процесса. Учитывают собираемую статистику, из которой выбирают прецеденты нарушений. Для задаваемого периода прогноза расчетные значения рисков, свойственные состоявшимся нарушениям, определяют как недопустимые, а меньшие по сравнению с недопустимыми определяют как допустимые (этим значениям рисков соответствует прецедентное отсутствие нарушений требований по защите информации). Для этого периода прогноза во множестве расчетных значений допустимых рисков выбирают максимальное значение. Поскольку это значение допустимого риска отвечает задаваемым условиям функционирования системы согласно принятой модели угроз безопасности информации и априори является приемлемым для заинтересованных сторон, его признают в качестве допустимого по факту прецедента. Это значение допустимого риска устанавливают в качестве нормы эффективности защиты информации по прецедентному принципу и используют для формального решения задач системного анализа.

Примечания

1 При отсутствии собственной статистики допускается использование статистики для похожих систем, в том числе из разных областей приложения. Применительно к системному анализу рисков такие системы рассматриваются как аналоги.

2 Альтернативным прецедентному принципу считают выбор допустимого риска при ориентации на систему-эталон (см. приложение Д).

7.4 Требования к выявлению явных и скрытых угроз

7.4.1 Выявление явных и скрытых угроз направлено на раннее распознавание и оценку развития предпосылок к нарушению требований по защите информации и надежности выполнения рассматриваемого процесса.

7.4.2 Выявление явных и скрытых угроз в рассматриваемом процессе осуществляют по результатам анализа различных факторов, воздействующих на защищаемую информацию, источников угроз и прогнозирования рисков.

Для выявления явных и скрытых угроз используют следующие процедуры:

1) при анализе на уровне конкретного множества выходных результатов процесса в сравнении с допустимым риском нарушения требований по защите информации — выявление явных и скрытых угроз осуществляют путем сравнения прогнозируемого риска с установленным допустимым риском. Множество выходных результатов, для которого значение прогнозируемого риска нарушения требований по защите информации превышает допустимый уровень, характеризуют наличием признаков потенциально существенных угроз (согласно используемой модели угроз безопасности информации), способных привести за период прогноза к нарушению требований по защите информации. В этом случае рекомендуется дополнительный системный анализ возможных сценариев развития потенциально существенных угроз. Непревышение допустимого риска интерпретируют как соблюдение условий по удержанию риска в допустимых пределах для получения множества выходных результатов в течение периода прогноза или как несущественность рассматриваемых угроз;

2) при анализе на уровне конкретного выходного результата в сравнении с другими выходными результатами:

- если при получении сравниваемых выходных результатов были использованы одинаково защищаемые активы для отличающихся моделей угроз — выявление явных и скрытых угроз осуществляют путем сравнения прогнозируемых рисков нарушения требований по защите информации. Те угрозы (согласно используемой модели угроз), для которых значение прогнозируемого риска превышает средний уровень среди сравниваемых вариантов, характеризуют как потенциально существенные угрозы. В этом случае рекомендуется дополнительный системный анализ возможных сценариев развития потенциально существенных угроз;

- если при получении сравниваемых выходных результатов были использованы активы, защищаемые по-разному для совпадающих или отличающихся моделей угроз, — выявление явных и скры-

тых угроз осуществляют путем сравнения прогнозируемых рисков нарушения требований по защите информации. Те активы и соответствующий выходной результат, для которого значение прогнозируемого риска превышает средний уровень среди сравниваемых вариантов, характеризуют наличием признаков потенциально существенных угроз (согласно используемой модели угроз). В этом случае рекомендуется дополнительный системный анализ возможных сценариев развития потенциально существенных угроз;

3) при анализе на уровне конкретного множества действий процесса в сравнении с допустимым риском нарушения надежности реализации процесса с учетом требований по защите информации — выявление явных и скрытых угроз осуществляют путем сравнения прогнозируемого риска с установленным допустимым риском. Множество действий процесса, для которых значение прогнозируемого риска нарушения надежности реализации процесса с учетом требований по защите информации превышает допустимый уровень, характеризуют наличием признаков потенциально существенных угроз, способных привести к нарушению надежности выполнения процесса (согласно используемой модели угроз). Непревышение допустимого риска интерпретируют как соблюдение условий по удержанию риска в допустимых пределах для надежной реализации процесса в течение периода прогноза или как несущественность рассматриваемых угроз.

Примечание — Если в приложении к анализируемой системе все расчетные риски не превышают установленных допустимых рисков, то это означает, что результаты моделирования подтверждают удержание рисков в допустимых пределах, несущественность или отсутствие явных и скрытых угроз в течение всего периода прогноза. Если все расчетные риски превышают максимально допустимые, это означает высокую уязвимость анализируемой системы с точки зрения обеспечения защиты информации для установленных допустимых рисков.

Противодействие выявленным угрозам по результатам системного анализа осуществляют согласно ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, [21] — [24] с учетом специфики системы и реализуемой стадии ее жизненного цикла.

7.5 Требования к поддержке принятия решений

7.5.1 Прогнозирование рисков, обоснование допустимых рисков, обоснование эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах, выявление явных и скрытых угроз осуществляют для поддержки принятия решений:

- по обеспечению выполнения рассматриваемого процесса и нормы эффективности защиты информации;
- по обоснованию мер, направленных на достижение целей рассматриваемого процесса, противодействие угрозам и определение сбалансированных решений по защите информации при средне- и долгосрочном планировании;
- по обоснованию предложений по совершенствованию и развитию системы защиты информации.

Определяемые при этом допустимые риски играют роль ограничений для обеспечения эффективности защиты информации и формального решения задач, связанных с выявлением явных и скрытых угроз, обоснованием мер, направленных на достижение целей процессов, противодействие угрозам и определение сбалансированных решений по защите информации при средне- и долгосрочном планировании, с обоснованием предложений по совершенствованию и развитию системы защиты информации. В зависимости от целей решаемых задач допустимый риск связывают с заранее определенным периодом прогноза, моделями угроз, условиями и возможным ущербом, ожидаемым для этого периода прогноза.

7.5.2 Поддержка принятия решений по обеспечению выполнения рассматриваемого процесса основана на прогнозировании риска нарушения надежности реализации процесса и должна учитывать требования по защите информации (см. 7.2, 7.3, приложение В). Это позволит определить нормы эффективности защиты информации и решать задачи по выявлению явных и скрытых угроз (см. 7.4).

7.5.3 Поддержка принятия решений по обоснованию мер, направленных на достижение целей рассматриваемого процесса и противодействие угрозам, основана на предварительных действиях. Следует заранее определить меры, направленные на обеспечение надежности реализации процесса, выполнение требований по защите информации, выявление явных и скрытых угроз и на восстановление приемлемых условий выполнения процесса в случае выявления предпосылок к нарушению или непосредственно нарушений требований по защите информации. Определение этих мер защиты информации осуществляют согласно рекомендациям 4.3. Определение мер по обеспечению надежности

реализации процесса осуществляют по ГОСТ IEC 61508-3, ГОСТ Р ИСО 9000, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57272.1, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы и реализуемой стадии ее жизненного цикла.

Для обоснования мер, направленных на достижение целей системных процессов по ГОСТ Р 57193, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357 и противодействие угрозам, используют модели, методы и методики системного анализа и методические указания по прогнозированию рисков (см. приложения В, Г, Д, Е).

Причины наступления событий, связанных с выявленными предпосылками к нарушению требований по защите информации, явными и скрытыми угрозами, произошедшими нарушениями в процессах, регистрируют для недопущения подобных повторений и/или уточнения предупреждающих мер, обеспечения приемлемых условий выполнения процессов и наполнения базы знаний.

7.5.4 Поддержка принятия сбалансированных решений по защите информации при среднесрочном планировании основана на системном анализе значений расчетных показателей рисков при сроке прогноза от недели или месяца до одного года, при долгосрочном — от одного года до нескольких лет с учетом специфики системы.

При недопустимых значениях прогнозируемых рисков и/или при наступлении реальных нарушений в рассматриваемом процессе должны быть выявлены их причины и определены меры для целенаправленного планового восстановления надежности выполнения процесса на уровне рисков, не превышающих допустимые.

Примечание — Баланс по критерию «эффективность — стоимость» при средне- и долгосрочном планировании должен достигаться с использованием процесса системного анализа.

Для обоснования сбалансированных решений по защите информации при средне- и долгосрочном планировании используют модели, методы и методики системного анализа и методические указания по прогнозированию рисков (см. приложения В, Г, Д, Е).

7.5.5 Поддержка принятия решений по обоснованию предложений по совершенствованию и развитию системы защиты информации основана на изучении результатов системного анализа значений расчетных показателей рисков при сроке прогноза от нескольких месяцев до нескольких лет. Реализация этих предложений должна быть учтена в долгосрочных планах организации.

Примечание — Эффективность вырабатываемых путей совершенствования и развития системы защиты информации должна достигаться с использованием базы знаний и процесса системного анализа.

Для обоснования предложений по совершенствованию и развитию системы защиты информации используют модели, методы и методики системного анализа и методические указания по прогнозированию рисков (см. приложения В, Г, Д, Е).

Примечание — Примеры постановки некоторых задач в процессе системного анализа приведены в приложении Г, а примеры решения задач системного анализа для других процессов проиллюстрированы в ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе системного анализа может включать (в части, свойственной этому процессу):

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

Приложение Б
(справочное)

Пример перечня угроз

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

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 58412;
- 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 возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному заказчику, информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Общие положения

Процесс системного анализа применим ко всем системным процессам (к процессам соглашения, процессам организационного обеспечения проекта, процессам технического управления, техническим процессам) по ГОСТ Р 57193, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, в том числе непосредственно к себе самому. Для прогнозирования различных рисков применимы любые научно обоснованные модели и методы, обеспечивающие приемлемое достижение поставленных целей.

В настоящем приложении приведены ссылки на стандарты системной инженерии, содержащие рекомендации по типовым моделям, методам и необходимым исходным данным для прогнозирования рисков во всех системных процессах (см. В.2).

Применимые для процесса системного анализа специальные положения по прогнозированию риска нарушения надежности реализации процесса, риска нарушения требований по защите информации и интегрального риска изложены в В.3.

В.2 Ссылки на типовые модели и методы

Ссылки на стандарты системной инженерии, содержащие рекомендации по типовым моделям, методам и необходимым исходным данным для прогнозирования рисков при проведении системного анализа, отражены в таблице В.1.

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

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

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые модели и методы
Процесс управления человеческими ресурсами системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59333—2021, приложение В
Процесс управления качеством системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59334—2021, приложение В
Процесс управления знаниями о системе	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59335—2021, приложение В
Процесс планирования проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59336—2021, приложение В
Процесс оценки и контроля проекта	По ГОСТ Р 59337—2021, подраздел 6.3	ГОСТ Р 59337—2021, приложение В
Процесс управления решениями	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59338—2021, приложение В
Процесс управления рисками для системы	По ГОСТ Р 59339—2021, подраздел 6.3	ГОСТ Р 59339—2021, приложение В
Процесс управления конфигурацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59340—2021, приложение В
Процесс управления информацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59341—2021, приложение В

Продолжение таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые модели и методы
Процесс измерений системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59342—2021, приложение В
Процесс гарантии качества для системы	По ГОСТ Р 59343—2021, подраздел 6.3	ГОСТ Р 59343—2021, приложение В
Процесс анализа бизнеса или назначения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59344—2021, приложение В
Процесс определения потребностей и требований заинтересованной стороны для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59345—2021, приложение В
Процесс определения системных требований	Частные показатели риска реализации угроз безопасности информации в условиях отсутствия мер защиты информации, предлагаемых к использованию в процессе; частные показатели риска реализации угроз безопасности информации в случае применения мер защиты информации, предлагаемых к использованию в процессе; интегральный риск нарушения функционирования системы и утечки защищаемой информации при применении мер защиты информации, предлагаемых к использованию в процессе; показатель риска нарушения надежности реализации процесса определения системных требований в части защиты информации	ГОСТ Р 59346—2021, приложения В, Д
Процесс определения архитектуры системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59347—2021, приложение В
Процесс определения проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59348—2021, приложение В
Процесс системного анализа	По 6.3	Настоящий стандарт, приложение В

Окончание таблицы В.1

Системный процесс	Вероятностные показатели риска	Ссылки на типовые модели и методы
Процесс реализации системы	Риск нарушения надежности выполнения процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения выполнения процесса с учетом требований по защите информации	ГОСТ Р 59350—2021, приложение В
Процесс комплексирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59351—2021, приложение В
Процесс верификации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59352—2021, приложение В
Процесс передачи системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59353—2021, приложение В
Процесс аттестации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59354—2021, приложение В
Процесс функционирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59355—2021, приложение В
Процесс сопровождения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59356—2021, приложение В
Процесс изъятия и списания системы	Риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации	ГОСТ Р 59357—2021, приложение В

Примечание — Другие возможные показатели, модели и методы оценки рисков приведены 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 58045, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

В.3 Специальные положения по прогнозированию рисков для процесса системного анализа

В.3.1 Типовые модели и методы прогнозирования рисков обеспечивают вероятностную оценку следующих показателей:

- риска нарушения надежности реализации процесса системного анализа без учета требований по защите информации (см. В.3.2 — В.3.7, В.4);
- риска нарушения требований по защите информации в процессе системного анализа (см. В.5);
- интегрального риска нарушения надежности реализации процесса системного анализа с учетом требований по защите информации (см. В.6).

В.3.2 Для расчета показателей рисков исследуемые сущности процесса рассматривают в виде моделируемой системы простой или сложной структуры. Модели и методы системного анализа таких систем используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, данные собираемой и накапливаемой статистики по процессам и возможным условиям их реализации.

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

В.3.3 При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если…», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования моделируемой системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.3.4 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается целостность моделируемой системы, 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, действия процесса, а также иные сущности, подлежащие учету при системном анализе);
- 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, действий и/или защитных преград, предназначенных для воспрепятствования реализации угроз.

Обоснованное использование выбранных мер и защитных преград позволяет рассматривать их в качестве предупреждающих контрмер, нацеленных на обеспечение успешной реализации рассматриваемых процессов.

В.3.5 Математические модели для прогнозирования рисков в системе, представляемой в виде «черного ящика», приведены в В.4.1, В.4.2. Модель В.4.2 для прогнозирования рисков при отсутствии какого-либо контроля является частным случаем модели В.4.3 при использовании технологии периодического контроля. Модель В.4.2 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 там, где ответственные лица пренебрегают функциями контроля или не реагируют должным образом на результаты системного анализа.

В.3.6 Для систем сложной структуры применимы модели и методы, изложенные в В.4.4.

В.3.7 Изложение моделей в В.4 дано в контексте нарушения надежности реализации процесса системного анализа без учета требований по защите информации. Для адаптации математических моделей к контексту нарушения требований по защите информации в В.4.3 приведен инженерный способ 1, его применение продемонстрировано в В.5, В.6 и приложении Г.

В.3.8 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 МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

В.4 Математические модели для прогнозирования риска нарушения надежности реализации процесса системного анализа

В.4.1 Общие положения

В.4.1.1 Надежность реализации процесса системного анализа представляет собой свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях реализации. Выполнение требований по защите информации в В.4 не учитывается, их рассмотрение проведено в В.5 и В.6. Для каждого из рассматриваемых действий или выходных результатов, являющихся элементом в моделируемой системе простой или сложной структуры, возможны либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения этого действия или получения выходного результата.

В.4.1.2 В терминах моделируемой системы, состоящей из элементов, отождествляемых с выполняемыми действиями или получаемыми выходными результатами, под целостностью моделируемой системы понимается такое состояние элементов рассматриваемой системы, которое в течение задаваемого периода прогноза отвечает требованию обеспечения надежной реализации процесса системного анализа. С точки зрения вероятностного прогнозирования риска нарушения надежности реализации процесса (например, для отдельного действия или выходного результата как элемента моделируемой системы) пространство элементарных состояний на временной оси образуют следующие основные состояния:

- «Целостность элемента моделируемой системы сохранена», если в течение всего периода прогноза обеспечена надежная реализация анализируемого действия или получения определенного выходного результата процесса, при этом обеспечено требуемое качество используемой в системном анализе информации;
- «Целостность элемента моделируемой системы нарушена» — в противном случае.

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

Надежность реализации процесса системного анализа в течение задаваемого периода прогноза обеспечена, если в течение этого периода для всех недублируемых элементов моделируемой системы (например, для всех осуществляемых действий или получаемых выходных результатов или иных рассматриваемых сущностей, логически объединяемых условием «И») обеспечена их целостность, т. е. наблюдается элементарное состояние «Целостность элемента моделируемой системы сохранена».

В.4.2 Математическая модель «черного ящика» при отсутствии какого-либо контроля

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

Модель представляет собой частный случай модели В.4.3, если период между контролями состояния системы больше периода прогноза. Учитывая это, используют формулы (В.1) — (В.5) из В.4.3.

В.4.3 Математическая модель «черного ящика» при использовании технологии периодического контроля

В моделируемой системе, представленной в виде «черного ящика», осуществляется периодический контроль ее состояния с точки зрения надежности реализации процесса системного анализа.

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

В рамках модели развитие событий в системе считается не нарушающим надежность реализации процесса системного анализа в течение заданного периода прогноза, если к началу этого периода требуемые условия для реализации процесса обеспечены и в течение всего периода либо источники угроз не активизируются, либо после активизации происходит их своевременное выявление и принятие адекватных мер противодействия угрозам. В целях моделирования предполагают, что существуют не только средства контроля (диагностики) состояния реализуемого процесса системного анализа, но и способы поддержания и/или восстановления возможностей по выполнению процесса при выявлении источников или следов активизации угроз. Восстановление осуществляется лишь в период контроля (диагностики). Соответственно, чем чаще осуществляют контроль хода реализации процесса системного анализа с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии ненарушения надежности его реализации из-за возможных угроз (т. к. нарушения устраняют за счет предупреждающих действий по результатам системной диагностики состояния моделируемой системы и выявления при диагностике предпосылок к нарушениям, отдаляя тем самым непосредственно момент нарушения).

За основу анализа принят следующий последовательный алгоритм возникновения потенциально существенной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться, представляя угрозу для нарушения надежности реализации процесса системного анализа. По прошествии периода активизации, свойственного этой угрозе (в общем случае этот период активизации представляет собой случайную величину), наступает виртуальный момент нарушения, интерпретируемый как момент реализации угрозы, т. е. нарушения надежности реализации процесса системного анализа с возможными негативными последствиями.

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

Надежность реализации процесса системного анализа считается нарушенной лишь после того, как активизация источника угрозы происходит за период прогноза (т. е. возникает элементарное состояние «Целостность элемента моделируемой системы нарушена»). При отсутствии нарушений результатом применения очередной системной диагностики является подтверждение возможностей по реализации процесса, а при наличии нарушений перед диагностикой результатом применения очередной системной диагностики является полное восстановление нарушенных возможностей реализации процесса (до приемлемого уровня).

С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения надежности реализации процесса системного анализа 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 надежности реализации процесса системного анализа в течение заданного периода прогноза при использовании технологии периодического контроля (диагностики). При этом учитываются предпринимаемые меры и действия периодической диагностики и восстановления возможностей по реализации процесса.

Для расчета риска нарушения надежности реализации процесса системного анализа применительно к анализируемой системе исходные данные формально определяют по отношению к выполняемым действиям процесса и защищаемым активам (при необходимости исходные данные переопределяют или детализируют):

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

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

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

$T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы;

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

Примечание — Возможные переопределения этих исходных данных (согласно инженерному способу 1 из В.4.4), конкретизированные в приложении к выходным результатам и действиям процесса, приведены в приложении Г.

Оценку вероятности нарушения надежности реализации процесса $R_{надежн}(T_{зад})$ в течение периода прогноза $T_{зад}$ осуществляют 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 отсутствия нарушений надежности реализации процесса в системе в течение периода $T_{зад}$.

Возможны два варианта:

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

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

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

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

Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия нарушений требований по защите информации в моделируемой системе в течение прогноза $T_{зад}$ вычисляют по формуле

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

где $P_{серед}$ — вероятность отсутствия нарушений требований по защите информации в системе в течение всех периодов между системными контролями, целиком вошедшими в границы времени $T_{зад}$, вычисляемая по формуле

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

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

$P_{кон}$ — вероятность отсутствия нарушений по защите информации после последнего системного контроля в конце периода прогноза до истечения времени $T_{зад}$, вычисляемая по формуле (В.2), т. е.

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

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

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

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

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

В итоге вероятность отсутствия нарушений надежности реализации процесса системного анализа 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 системного анализа $R_{надежн}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического контроля и восстановления возможностей по выполнению процесса. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения надежности реализации процесса системного анализа в течение заданного периода прогноза при использовании технологии периодического контроля.

Примечание — В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель В.4.3 превращается в модель В.4.2 для прогноза риска нарушения надежности реализации процесса системного анализа при отсутствии какого-либо контроля.

В.4.4 Расчет риска для систем сложной структуры, комбинация и повышение адекватности моделей

Описанные в В.4.2 и В.4.3 модели применимы для проведения оценок, когда система представляется в виде «черного ящика» и значения времен системной диагностики и восстановления нарушенной целостности совпадают. В развитие моделей В.4.2 и В.4.3 в настоящем подразделе приведены способы, позволяющие создание моделей для систем сложной структуры и более общего случая — когда значения времен системной диагностики и восстановления нарушенных возможностей системы различны.

Расчет основан на применении следующих инженерных способов.

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

2-й способ позволяет переходить от оценок систем или отдельных элементов, представляемых в виде «черного ящика», к оценкам систем сколь угодно сложной параллельно-последовательной логической структуры. В формируемой структуре, исходя из реализуемых технологий для системы, состоящей из двух элементов, взаимовлияющих на выполнение процесса, указывается характер их логического соединения. Если два элемента

соединяются последовательно, что означает логическое соединение «И» (см. рисунок В.1), то в контексте надежности реализации процесса это интерпретируется так: «в системе обеспечена надежность реализации процесса в течение времени *t*, если «И» 1-й элемент, «И» 2-й элемент сохраняют свои возможности по надежной реализации процесса в течение этого времени». Если два элемента соединяются параллельно, что означает логическое соединение «ИЛИ» (см. рисунок В.2), это интерпретируется так: «система сохраняет возможности по надежной реализации процесса в течение времени *t*, если «ИЛИ» 1-й элемент, «ИЛИ» 2-й элемент сохраняют свои возможности по надежной реализации процесса в течение этого времени».

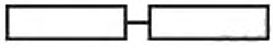


Рисунок В.1 — Система из последовательно соединенных элементов («И»)

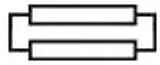


Рисунок В.2 — Система из параллельно соединенных элементов («ИЛИ»)

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

а) для системы из двух последовательно соединенных элементов

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

б) для системы из двух параллельно соединенных элементов

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

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

Рекурсивное применение соотношений (В.6), (В.7) снизу вверх дает соответствующие вероятностные оценки для сколь угодно 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.4.2 или В.4.3 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 подсистем. И так — до объединения на уровне системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (В.6) или (В.7) от исходных параметров моделей В.4.2 и В.4.3.

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.4.2 и В.4.3 и применения 2-го способа получается вероятность нарушения надежности реализации процесса в течение заданного периода времени *t*. Если для каждого элемента просчитать эту вероятность для всех точек *t* от нуля до бесконечности, получится траектория функции распределения времени нарушения надежности реализации процесса по каждому из элементов в зависимости от реализуемых мер контроля и восстановления целостности, т. е. то, что используется в формулах (В.6) и (В.7). Полученный вид этой функции распределения, построенной по точкам (например, с использованием программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения надежности реализации процесса каждого из элементов и моделируемой системы в целом. С точки зрения системной инженерии это среднее время интерпретируют как виртуальную среднюю наработку на нарушение надежности реализации процесса системного анализа при прогнозировании риска по моделям В.4.2 и В.4.3 для системы простой и сложной структуры. Обратная величина этого среднего времени является частотой нарушений надежности реализации процесса системного анализа в условиях определенных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения процесса для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей В.4.2 и В.4.3 или аналогичных им для расчетов по моделям «черного ящика». Этот способ используют, когда изначальной статистики для определения частоты нет или ее недостаточно.

4-й способ в дополнение к возможностям 2-го и 3-го способов повышает адекватность моделирования за счет развития моделей В.4.2 и В.4.3 в части учета времени на восстановление после нарушения надежности реа-

лизации процесса. В моделях В.4.2 и В.4.3 время системного контроля по составному элементу одинаково и равно в среднем $T_{диаг}$. Вместе с тем если по результатам контроля требуются дополнительные меры для восстановления нарушенных возможностей по выполнению процесса в течение времени $T_{восст}$, то для расчетов усредненное время контроля $T_{диаг}$ должно быть увеличено (если $T_{диаг} < T_{восст}$) или уменьшено (если $T_{диаг} > T_{восст}$) с учетом частоты восстановлений. При этом усредненное время контроля вычисляют итеративно с заданной точностью:

- 1-я итерация определяет время $T_{диаг}^{(1)} = T_{диаг}$, задаваемое на входе модели. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемых возможностей по выполнению процесса (т. е. в рамках времени диагностики);
- 2-я итерация осуществляется после расчета риска $R^{(1)}$ по исходным данным после 1-й итерации

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

где $R^{(1)}$ — риск нарушения целостности моделируемой системы с исходным значением $T_{диаг}^{(1)}$, вычисляемый с использованием моделей В.2.2, В.2.3. Поскольку на 1-й итерации время $T_{диаг}^{(1)}$ не учитывает времени восстановления, риск $R^{(1)}$, рассчитываемый с использованием модели В.2.3, начинает приближаться к реальному;

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

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

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

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

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 нарушаемой целостности моделируемой системы.

При этом для расчетов применяются одни и те же модели подразделов В.4.2 и В.4.3.

Примечание — Способ итеративного применения процессов рекомендован ГОСТ Р 57102.

Применение инженерных способов 1—4 обеспечивает более точный прогноз для системы сложной структуры.

В.4.5 Учет качества используемой информации

В случае критичности качества используемой информации для принятия решений в приложении к моделируемой системе действие сбора и анализа качества информации рассматривают отдельно. При этом дополнительно применяют модели и методы оценки качества выходной информации по ГОСТ Р 59341. Итоговую вероятность нарушения надежности реализации процесса системного анализа $R_{надежн}(T_{зад})$ в течение периода прогноза $T_{зад}$, без учета требований по защите информации вычисляют по формуле

$$R_{надежн}(T_{зад}) = 1 - [1 - R_{надежн\ В.4.2—В.4.3}(T_{зад})] \cdot [1 - R_{наруш.\ УИ}(T_{зад})], \quad (В.10)$$

где $R_{надежн\ В.4.2—В.4.3}(T_{зад})$ — вероятность нарушения надежности реализации процесса системного анализа в течение периода прогноза Тзад без учета качества используемой информации и требований по защите информации, вычисляемая по моделям и рекомендациям В.4.2, В.4.3;

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

В.5 Математические модели для прогнозирования риска нарушения требований по защите информации

В.5.1 Общие положения

В.5.1.1 Прогнозирование риска нарушения требований по защите информации осуществляют на основе применения математических моделей для прогнозирования риска нарушения требований по защите информации из ГОСТ Р 59341—2021 (В.2 приложения В). Все положения по моделированию, изложенные в ГОСТ Р 59341 применительно к процессу управления информацией, в полной мере применимы к процессу системного анализа (в части, свойственной прогнозированию риска нарушения требований по защите информации). Для расчета типовых показателей рисков анализируемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. В моделях и методах системного анализа применительно к таким моделируемым системам используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики по процессу и возможным условиям его реализации.

Примечание — Поскольку для прогнозирования риска нарушения требований по защите информации в процессе системного анализа могут быть использованы те же модели из В.4.2 — В.4.4 (изложенные в контексте анализа надежности), в В.5.1.2 — В.5.1.6 продемонстрировано применение инженерного способа 1 из В.4.4, позволяющее проводить расчеты в контексте развития и реализации угроз безопасности информации.

В.5.1.2 В моделях простой структуры под анализируемой системой понимают определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявлены требования и выполняют меры защиты информации. Система простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединенных для анализа как один элемент. Анализ системы простой структуры осуществляют по принципу «черного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы. Система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых представляется в виде «черного ящика», функционирующего в условиях неопределенности.

В.5.1.3 При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если...», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.5.1.4 Для математической формализации используют следующие основные положения:

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

Под целостностью моделируемой системы понимается такое ее состояние, которое в течение задаваемого периода прогноза отвечает целевому назначению модели системы. В данном случае непосредственно процесс системного анализа может быть рассмотрен в качестве моделируемой системы. При моделировании, направленном на прогнозирование риска нарушения требований по защите информации, целевое назначение моделируемой системы проявляется в выполнении требований по защите информации. Такая интерпретация подразумевает выполнение требований по защите информации не только применительно к защищаемым активам и действиям, с использованием которых создают и получают выходные результаты, но и к самим выходным результатам, которые применяют (или планируют к созданию, получению и/или применению). В итоге для каждого из элементов и моделируемой системы в целом в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси 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.

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

В.5.1.5 В моделях простой структуры 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 техно-

логии системного контроля выполнения требований по защите информации и восстановления системы после состоявшихся нарушений или выявленных предпосылок к нарушениям. В моделях сложной структуры под моделируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логически представляет собой определенное действие или выходной результат и совокупность задействованных активов, к которым предъявлены требования и применяют меры защиты информации. При этом выходной результат сам может стать активом в итоге выполняемых действий.

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

В.5.1.6 При расчетах с использованием математических моделей для прогнозирования риска нарушения требований по защите информации и рекомендаций ГОСТ Р 59341—2021 (В.2, В.3 приложения В) осуществляют учет предпринимаемых мер периодической диагностики и восстановления возможностей по обеспечению выполнения требований по защите информации. В результате математического моделирования рассчитывают вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение до единицы, представляющее собой вероятность нарушения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе нарушено»). В свою очередь вероятность нарушения требований по защите информации в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения требований по защите информации в процессе системного анализа.

В.5.2 Исходные данные и расчетные показатели

Для расчета вероятностных показателей применительно к моделируемой системе используют исходные данные, формально определяемые в общем случае следующим образом:

σ — частота возникновения источников угроз безопасности информации в процессе системного анализа;

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 требований по защите информации в моделируемой системе в течение периода $T_{зад}$;

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

Расчет показателей применительно к процессу системного анализа 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 $R_{наруш}(T_{зад}) = R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ для процесса системного анализа в течение периода прогноза осуществляют как дополнение до единицы значения $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$.

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

В.6 Прогнозирование интегрального риска нарушения надежности реализации процесса с учетом требований по защите информации

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

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

где $R_{надежн}(T_{зад})$ — вероятность нарушения надежности реализации процесса системного анализа в течение периода прогноза $T_{зад}$ без учета требований по защите информации, вычисляемая по моделям и рекомендациям В.3, В.4;

$R_{наруш}(T_{зад})$ — вероятность нарушения требований по защите информации в системе для процесса системного анализа в течение периода прогноза $T_{зад}$, вычисляемая по моделям и рекомендациям В.5.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса системного анализа

Г.1 Общие положения

Настоящие методические указания содержат дополнительные разъяснения относительно прогнозирования рисков в процессе системного анализа с ориентацией на защиту информации. Расчетные значения рисков на заданный период прогноза используют для решения задач системного анализа (см. раздел 7). При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможным ущербом. В общем случае решение задач системного анализа направляют на более детальное понимание функциональных возможностей системы и ее результативности, на контроль состояния эксплуатационной среды, прогнозирование рисков и определение допустимых рисков, выявление явных и скрытых угроз, оценку и обоснование стратегий, технического облика и сбалансированных системных решений и планов, сравнение альтернатив, выработку критериев и осуществление прогноза безопасности, обеспечение качества и эффективности системы для задаваемых условий, выработку требований к характеристикам и показателям функционирования системы, оценку свойств и критичности влияния различных параметров на поведение системы, рациональную настройку параметров, разрешение противоречий и поддержание устойчивости функционирования системы.

Примечание — Дополнительно могут быть востребованы методики по оценке ущербов, учитывающие специфику системы (см., например, ГОСТ Р 22.10.01, ГОСТ Р 54145).

Г.2 Анализируемые объекты

Применительно к конкретной рассматриваемой системе согласно 4.3, 5.3, 6.1 определению подлежат:

- основные элементы и логическая структура рассматриваемой системы, подлежащие системному анализу;
- состав заинтересованных сторон, имеющих интерес к рассматриваемой системе;
- состав выходных результатов, выполняемых действий процесса системного анализа и используемых при этом активов;
- перечень угроз и возможные сценарии возникновения и развития угроз для выходных результатов и выполняемых действий процесса системного анализа;
- иные объекты, используемые для прогнозирования рисков, при необходимости оценки того, насколько организация процесса системного анализа способна обеспечить возможности по его выполнению и достижение целей процесса.

При проведении системного анализа других системных процессов анализируемые объекты определяют по ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357.

Г.3 Цель прогнозирования рисков

Основной целью прогнозирования рисков для рассматриваемой системы является установление степени вероятного нарушения требований по защите информации и/или нарушения надежности реализации исследуемых системных процессов (процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления, технических процессов) с учетом требований по защите информации за заданный период прогноза. Прогнозирование рисков осуществляют в интересах решения определенных задач системного анализа (см. раздел 7). Конкретные практические цели прогнозирования рисков устанавливает заказчик системного анализа и/или аналитик моделируемой системы при выполнении работ системной инженерии.

Г.4 Рекомендуемые модели и методы

Для решения задач системного анализа, связанных с оценкой вероятностных показателей рисков, используют модели и методы, рекомендуемые в приложении В.

Синергетические эффекты системного анализа достигаются за счет количественно обоснованного целенаправленного уменьшения различных рисков при реализации каждого из процессов соглашения, организационного обеспечения проекта, технического управления и технических процессов на всех этапах жизненного цикла рассматриваемых систем.

Г.5 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе исходными данными являются данные, необходимые для проведения расчетов по моделям и методам, рекомендуемым в приложении В.

Г.6 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

Шаг 1. Устанавливают анализируемые объекты и определяют рассматриваемую и моделируемые системы для прогнозирования рисков (см. Г.2).

Шаг 2. Определяют конкретные цели прогнозирования и решаемые задачи системного анализа (см. Г.3).

Шаг 3. Формируют перечень возможных угроз, выделяя угрозы нарушения требований по защите информации. Принимают решение о представлении каждой из моделируемых систем 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. Выбирают расчетные показатели и подходящие математические модели и методы (см. Г.4, Г.5).

Шаг 4. Разрабатывают необходимые методики системного анализа, опирающиеся на выбранные модели и методы (см. приложение Е). Осуществляют математическое моделирование, завершаемое расчетом выбранных показателей согласно моделям и методикам системного анализа.

Шаг 5. Результаты расчетов применяют для достижения поставленных целей (см. Г.3).

Примечание — В случае изначального наличия только вербального описания системы проводят его логическое преобразование к виду, позволяющему осуществить формальные постановки задач системного анализа (см. пример в Г.8).

Г.7 Обработка и использование результатов прогнозирования рисков для постановки и решения задач системного анализа

Результаты прогнозирования рисков должны быть удобны заказчику и/или аналитику моделируемой системы для постановки и формального решения задач системного анализа. Результаты представляются в виде гистограмм, графиков, таблиц и/или в ином виде, позволяющем анализировать зависимости рисков от изменения значений исходных данных при решении задач системного анализа. Результаты расчетов подлежат использованию для решения задач системного анализа (см. раздел 7 и приложение Е).

В таблице Г.1 представлены возможные цели для постановок задач системного анализа применительно к каждому из системных процессов и используемых вероятностных показателей рисков, моделей и методов из таблицы В.1. Их применение позволяет осуществить формальные постановки задач системного анализа с использованием моделей и методов, рекомендуемых настоящим стандартом и ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357.

Таблица Г.1 — Возможные цели в постановках задач системного анализа

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процессы приобретения и поставки продукции и услуг для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса приобретения и поставки продукции и услуг для системы; - ненарушения сроков поставки продукции и/или услуг; - непревышения уровня допустимого брака в поставляемых продукции и/или услугах
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе приобретения и поставки продукции и услуг для системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск;

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
		- период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе приобретения и поставки продукции и услуг для системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процессов приобретения и поставки продукции и услуг для системы и защите информации в этих процессах, приводящие к удержанию рисков в допустимых пределах
Процесс управления моделью жизненного цикла системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса управления моделью жизненного цикла системы; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления моделью жизненного цикла системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления моделью жизненного цикла системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления моделью жизненного цикла системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления инфраструктурой системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения надежности реализации процесса управления инфраструктурой системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления инфраструктурой системы

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления инфраструктурой системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления инфраструктурой системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления инфраструктурой системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления портфелем проектов	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса управления портфелем проектов; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления портфелем проектов (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления портфелем проектов
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления портфелем проектов и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процесс управления человеческими ресурсами системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения надежности реализации процесса управления человеческими ресурсами системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления человеческими ресурсами системы
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления человеческими ресурсами системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления человеческими ресурсами системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления человеческими ресурсами системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления качеством системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса управления качеством системы; - ненарушения сроков поставки продукции и/или услуг; - непревышения уровня допустимого брака в поставляемых продукции и/или услугах
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления качеством системы (если это возможно при управлении рисками);

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
		- увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления качеством системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления качеством системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления знаниями о системе	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса приобретения знаний; - ненарушение сроков поставки приобретаемых знаний; - непревышение уровня допустимого брака в приобретаемых знаниях. Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса создания полезных знаний; - ненарушение сроков создания полезных знаний; - непревышение уровня допустимого брака в создаваемых знаниях
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления знаниями о системе
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления знаниями о системе и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процесс планирования проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса планирования проекта; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе планирования проекта (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе планирования проекта
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса планирования проекта и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс оценки и контроля проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса оценки и контроля проекта; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе оценки и контроля проекта (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе оценки и контроля проекта

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса оценки и контроля проекта и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления решениями	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения надежности реализации процесса управления решениями (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления решениями
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления решениями (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления решениями
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления решениями и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления рисками для системы	Риски по ГОСТ Р 59339	Обосновать для задаваемых ограничений способы уменьшения рисков или удержания рисков в допустимых пределах (показатели рисков — по ГОСТ Р 59339)
Процесс управления конфигурацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса управления конфигурацией системы; - ненарушения сроков выполнения необходимых действий процесса

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления конфигурацией системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе управления конфигурацией системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления конфигурацией системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс управления информацией системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - обеспечения необходимой надежности представления используемой информации; - обеспечения необходимой своевременности представления используемой информации; - обеспечения необходимой полноты оперативного отражения в системе новых объектов и явлений; - обеспечения необходимой актуальности обновляемой информации; - обеспечения необходимой безошибочности информации после контроля; - обеспечения необходимой корректности обработки информации; - обеспечения необходимой безошибочности действий должностных лиц
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе управления информацией системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия.

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
		Обосновать для задаваемых ограничений рациональные способы: - сохранения целостности информации системы в условиях опасных программно-технических воздействий; - обеспечения защищенности активов от несанкционированного доступа; - сохранения конфиденциальности используемой информации
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса управления информацией системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс измерений системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса измерений системы; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе измерений системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе измерений системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса измерений системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс гарантии качества для системы	Риски по ГОСТ Р 59343	Обосновать для задаваемых ограничений способы уменьшения рисков или удержания рисков в допустимых пределах (показатели рисков — по ГОСТ Р 59343)
Процесс анализа бизнеса или назначения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса анализа бизнеса или назначения системы; - ненарушения сроков выполнения необходимых действий процесса

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе анализа бизнеса или назначения системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе анализа бизнеса или назначения системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса анализа бизнеса или назначения системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс определения потребностей и требований заинтересованной стороны для системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса определения потребностей и требований заинтересованной стороны для системы; - повышение готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения потребностей и требований заинтересованной стороны для системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процесс определения системных требований	Частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения	Обосновать для задаваемых ограничений способы: - защиты системы от вредоносного программного обеспечения; - межсетевого экранирования; - использования системы обнаружения вторжений и пресечения попыток проникновения в операционную среду; - применения мер разграничения доступа на территорию, к оборудованию и к информации в системе, в том числе мер идентификации и аутентификации пользователей и процессов; - применения средств и комплексов доверенной загрузки; - применение мер контроля и анализа защищенности программных и программно-аппаратных модулей системы от угроз изменения настроек и нарушения функционирования; - мониторинга, регистрации и учета действий пользователей и выполнения процессов в системе; - пресечения и блокирования неправомерных действий пользователей, в том числе направленных на несанкционированную инсталляцию программного обеспечения; - применения мер резервирования и восстановления программного и аппаратного обеспечения системы
	Частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения	Обосновать для задаваемых ограничений способы: - защиты системы от вредоносного программного обеспечения; - межсетевого экранирования; - использования системы обнаружения вторжений и пресечения попыток проникновения в операционную среду; - применения мер разграничения доступа на территорию, к оборудованию и к информации в системе, в том числе мер идентификации и аутентификации пользователей и процессов; - применения средств и комплексов доверенной загрузки; - применения мер контроля и анализа защищенности программных и программно-аппаратных модулей системы от угроз возможной утечки информации; - мониторинга, регистрации и учета действий пользователей и выполнения процессов в системе; - пресечения и блокирование неправомерных действий пользователей, направленных на копирование информации и/или несанкционированную ее передачу во внешние сети; - учета, регистрации и применения технических мер защиты отчуждаемых носителей информации; - применения криптографической защиты трафика как внутри системы, так и при взаимодействии ее с другими системами
	Интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях	Обосновать для задаваемых ограничений способы уменьшения рисков реализации угроз безопасности информации, оцениваемых по частным показателям (см. выше), а также способы: - мониторинга публикаций по возможным угрозам и инцидентам безопасности информации, новым уязвимостям системного и прикладного программного обеспечения и

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований	средствам их эксплуатации в интересах учета при формировании системных требований в части защиты информации на всех стадиях жизненного цикла системы; - согласования подлежащих применению на разных стадиях жизненного цикла системы мер защиты от угроз нарушения функционирования системы или утечки конфиденциальной информации; - обеспечения возможности корректировки состава и характеристик мер защиты от угроз нарушения функционирования системы или ее элементов и угроз утечки информации на каждой стадии жизненного цикла системы в зависимости от фактов нарушения безопасности информации, выявленных на предыдущих стадиях
Процесс определения архитектуры системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз надежности реализации процесса определения архитектуры системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения архитектуры системы
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе определения архитектуры системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения архитектуры системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса определения архитектуры системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процесс определения проекта	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса определения проекта; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе определения проекта (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе определения проекта
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса определения проекта и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс системного анализа	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения для каждого из системных процессов необходимых условий с завершением всех предпринимаемых действий, связанных с прогнозированием рисков, обоснованием допустимых рисков, выявлением явных и скрытых угроз, поддержкой принятия решений в жизненном цикле системы; - ненарушения сроков выполнения необходимых действий процесса; - удержания рисков в допустимых пределах
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе системного анализа (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения.

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
		Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе системного анализа
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса системного анализа и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс реализации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса реализации системы; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе реализации системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе реализации системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности выполнения процесса реализации системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс комплексирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса комплексирования системы; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе комплексирования системы (если это возможно при управлении рисками);

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
		- увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе комплексирования системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса комплексирования системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс верификации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса верификации системы; - ненарушения сроков выполнения необходимых действий процесса
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе верификации системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе верификации системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса верификации системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс передачи системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса передачи системы; - ненарушения сроков выполнения необходимых действий процесса

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе передачи системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе передачи системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса передачи системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс аттестации системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса аттестации системы; - обеспечение готовности системы к выполнению требований заинтересованных сторон по качеству, срокам и затратам
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе аттестации системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе аттестации системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса аттестации системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
Процесс функционирования системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения надежности реализации процесса функционирования системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе функционирования системы. Обосновать для задаваемых ограничений рациональные способы: - обеспечения необходимой надежности представления используемой информации; - обеспечения необходимой своевременности представления используемой информации; - обеспечения необходимой полноты оперативного отражения в системе новых объектов и явлений; - обеспечения необходимой актуальности обновляемой информации; - обеспечения необходимой безошибочности информации после контроля; - обеспечения необходимой корректности обработки информации; - обеспечения необходимой безошибочности действий должностных лиц
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе функционирования системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе функционирования системы; - сохранение целостности системы в условиях опасных программно-технических воздействий; - обеспечение защищенности активов от несанкционированного доступа; - сохранение конфиденциальности используемой информации

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса функционирования системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс сопровождения системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения надежности реализации процесса сопровождения системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе сопровождения системы
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе сопровождения системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе сопровождения системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса сопровождения системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах
Процесс изъятия и списания системы	Риск нарушения надежности реализации процесса без учета требований по защите информации	Обосновать для задаваемых ограничений рациональные способы: - выполнения необходимых условий с завершением всех предпринимаемых действий процесса изъятия и списания системы; - ненарушения сроков выполнения необходимых действий процесса

Окончание таблицы Г.1

Системный процесс	Вероятностные показатели рисков	Возможные цели в постановках задач системного анализа для использования методов и моделей из таблицы В.1
	Риск нарушения требований по защите информации в процессе	Обосновать для задаваемых ограничений рациональные способы: - снижения частоты возникновения источников угроз нарушения требований по защите информации в процессе изъятия и списания системы (если это возможно при управлении рисками); - увеличения времени развития угроз до нарушения (если это возможно при управлении рисками); - снижения длительности системной диагностики; - уменьшения времени восстановления системы после нарушения. Обосновать для задаваемых ограничений: - период времени между системными диагностиками, минимизирующий риск; - период прогноза, когда возможны эффективные предупреждающие управленческие воздействия в процессе изъятия и списания системы
	Интегральный риск нарушения надежности реализации процесса с учетом требований по защите информации	Обосновать для задаваемых ограничений сбалансированные действия по обеспечению надежности реализации процесса изъятия и списания системы и защите информации в процессе, приводящие к удержанию рисков в допустимых пределах

Г.8 Пример логического преобразования вербального описания системы для осуществления формальных постановок задач

Г.8.1 Нижеследующий пример призван продемонстрировать возможные способы логического преобразования вербального описания системы (см. [27], [28]) к такому виду, который позволит осуществить формальные постановки задач системного анализа (см. таблицу Г.1), используя модели и методы В.4. В качестве рассматриваемой системы в примере выступает технический облик гипотетичной многоуровневой системы управления рисками (СУР), подлежащей созданию в интересах обеспечения энергетической безопасности в Российской Федерации.

Г.8.2 Согласно «Доктрине энергетической безопасности Российской Федерации», (далее по тексту — Доктрина) и «Энергетической стратегии Российской Федерации на период до 2035 года» (см. [27], [28]), энергетика РФ вносит значительный вклад в национальную безопасность и социально-экономическое развитие страны. С учетом множества факторов неопределенности состоянию энергетической безопасности РФ присущи долговременные разнородные вызовы и угрозы. Основу энергетики РФ составляет топливно-энергетический комплекс (ТЭК), включающий в себя нефтяную, газовую, угольную и торфяную отрасли, электроэнергетику и теплоснабжение. Предприятия ТЭК образуют критическую информационную инфраструктуру и подлежат всесторонней защите от угроз информационной безопасности [15]. При реализации энергетической стратегии неизбежны неопределенности в специфике решения практических задач, требующих математического моделирования, прогнозирования рисков и системного анализа на различных мета-уровнях рассматриваемой системы СУР.

Для оценки состояния энергетической безопасности РФ используются различные критерии, связанные с преследуемыми целями. Эти цели могут быть различными для федерального уровня, уровня федеральных округов, макрорегионов или отдельно взятого субъекта энергетической безопасности. Таким образом заинтересованными сторонами, равно как и самостоятельными моделируемыми системами при решении задач системного анализа для СУР, могут выступать Российская Федерация в целом, федеральный округ, макрорегион или отдельно взятый субъект энергетической безопасности.

Набор применяемых критериев системного анализа должен опираться на доступную информацию для расчетов в СУР и позволять оценивать существующие и потенциально существенные угрозы и риски, обозначенные в Доктрине. Содержание каждого из критериев должно в полной мере отвечать преследуемой цели или совокупности целей и учитывать возможности прогнозирования динамики изменения состояния энергетической безопасности РФ во времени. Для реализации этих положений применимы методы и модели настоящего стандарта, в т. ч. пошаговое их применение согласно Г.6.

Г.8.3 Основная цель обеспечения энергетической безопасности РФ определена в пункте 22 Доктрины (далее используется обозначение цели от 22а) до 22о) в зависимости от конкретизации этих дефисов по тексту пункта 22 в Доктрине). Так, согласно Доктрине целью обеспечения энергетической безопасности является «поддержание

защищенности экономики и населения страны от угроз энергетической безопасности на уровне, соответствующем требованиям законодательства Российской Федерации, касающимся (см. [27]):

- 22а) воспроизводства минерально-сырьевой базы ТЭК;
- 22б) надежного и устойчивого обеспечения российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики;
- 22в) формирования запаса продукции организаций ТЭК в государственном материальном резерве и поддержания его на необходимом уровне;
- 22г) обеспечения технической доступности инфраструктуры ТЭК для различных групп потребителей и возможности оказания им услуг в сфере энергетики;
- 22д) регулирования цен (тарифов) на продукцию организаций ТЭК и услуги в сфере энергетики;
- 22е) осуществления инвестиционной деятельности в сфере энергетики, обеспечения защиты прав инвесторов, контроля за иностранными инвестициями в российские организации ТЭК, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства;
- 22ж) осуществления антимонопольного регулирования и развития конкуренции, включая развитие организованной (биржевой) торговли продукцией организаций ТЭК;
- 22з) обеспечения энергосбережения и повышения энергетической эффективности;
- 22и) обеспечения антитеррористической защищенности и безопасности инфраструктуры и объектов ТЭК, в том числе в условиях чрезвычайных ситуаций;
- 22к) обеспечения защищенности критической информационной инфраструктуры объектов ТЭК;
- 22л) осуществления экспорта продукции, технологий и услуг организаций ТЭК;
- 22м) ограничения отрицательного воздействия на окружающую среду и обеспечения экологической безопасности хозяйственной деятельности организаций ТЭК;
- 22н) защиты населения и территорий от чрезвычайных ситуаций, возникающих на объектах ТЭК;
- 22о) применения российских технологий, оборудования, материалов, программного обеспечения при реализации инвестиционных проектов в отраслях ТЭК на территории РФ».

Тем самым по результатам рассмотрения вербального описания системы определены заинтересованные стороны и цели системного анализа для СУР.

В рамках системного анализа СУР различают два типа критериев оценки:

1-й тип (анализ): критерии для решения задач анализа, в т. ч. связанных с прогнозированием рисков;

2-й тип (синтез): критерии для поддержки принятия решений по выработке рациональных упреждающих мер противодействия угрозам.

Далее по результатам изучения вербального описания системы для решения задач анализа определены следующие критерии 1-го типа (см. рисунок Г.1):

- критерий КА1 — критерий прогнозирования рисков перерастания вызовов энергетической безопасности в угрозы в течение задаваемого прогнозного периода времени в сравнении с допустимыми, что используется в отношении внешнеэкономических (см. п. 8 Доктрины), внешнеполитических (см. пп. 9—10 Доктрины), внутренних (см. п. 15 Доктрины) и трансграничных (см. п. 18 Доктрины) вызовов;
- критерий КА2 — критерий прогнозирования рисков реализации угроз энергетической безопасности или наступления обстоятельств, оказывающих отрицательное влияние на состояние энергетической безопасности (в зависимости от действий или бездействия субъектов энергетической безопасности) в течение задаваемого прогнозного периода времени в сравнении с допустимыми, что используется в отношении внешнеэкономических (см. пп. 11—12 Доктрины), внешнеполитических (см. п. 13 Доктрины), внутренних (см. п. 16 Доктрины) и трансграничных (см. п. 19 Доктрины) угроз с учетом последствий (см. п. 21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24—29 Доктрины);
- критерий КА3 — критерий прогнозирования интегрального риска реализации изначальных угроз энергетической безопасности и угроз, способных перерасти из вызовов, в течение задаваемого прогнозного периода времени в сравнении с допустимым уровнем, что используется в отношении внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8—21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24—29 Доктрины).

Введенные критерии связаны с прогнозированием соответствующих рисков. Согласно п. 4 Доктрины под риском в области энергетической безопасности понимается возможность перерастания вызова энергетической безопасности в угрозу, реализации угрозы энергетической безопасности или наступления иных обстоятельств, оказывающих отрицательное влияние на состояние энергетической безопасности, в зависимости от действий или бездействия субъектов энергетической безопасности. В количественном выражении эти риски в полной мере могут быть оценены сочетанием вероятности нанесения ущерба и тяжести этого ущерба согласно определению 3.1.12. Характеристика угроз, способных возникнуть из вызовов, отражена в таблице Г.2. В свою очередь характеристика рисков в области энергетической безопасности, связанных с разнородными угрозами, и последствий от возможной реализации угроз отражена в таблице Г.3. В этих таблицах введены соответствующие обозначения для последующей формализации постановок задач системного анализа.

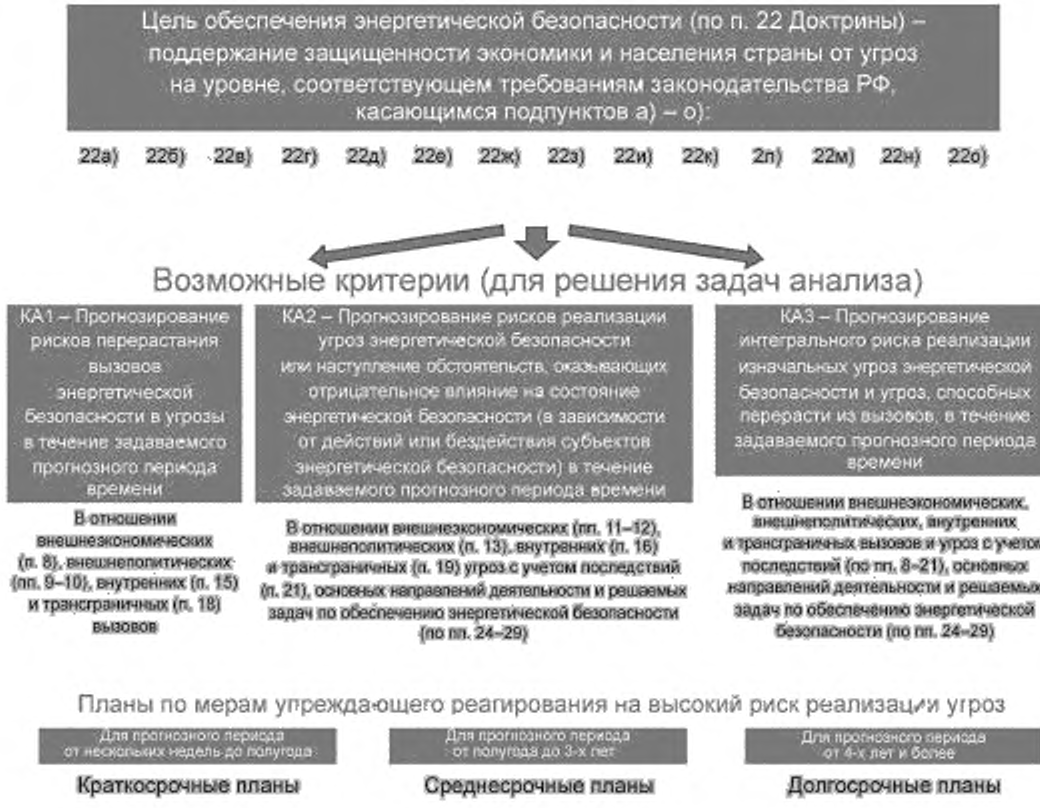


Рисунок Г.1 — Применимые критерии для решения задач анализа

Таблица Г.2 — Характеристика угроз, способных возникнуть из вызовов

Вызовы энергетической безопасности	Угрозы, способные возникнуть из вызовов
Внешнеэкономические вызовы (согласно п. 8 Доктрины): - ВнешЭВ8а) — перемещение центра мирового экономического роста в Азиатско-Тихоокеанский регион; - ВнешЭВ8б) — замедление роста мирового спроса на энергоресурсы и изменение его структуры, в том числе вследствие замещения нефтепродуктов другими видами энергоресурсов, развития энергосбережения и повышения энергетической эффективности; - ВнешЭВ8в) — увеличение мировой ресурсной базы углеводородного сырья, усиление конкуренции экспортеров энергоресурсов, в том числе в связи с появлением новых экспортеров;	Угрозы, способные возникнуть из внешнеэкономических вызовов: - ВнешЭВ-У8а) — угрозы, связанные с перемещением центра мирового экономического роста в Азиатско-Тихоокеанский регион; - ВнешЭВ-У8б) — угрозы, связанные с замедлением роста мирового спроса на энергоресурсы и изменением его структуры, в том числе вследствие замещения нефтепродуктов другими видами энергоресурсов, развития энергосбережения и повышения энергетической эффективности;

Окончание таблицы Г.2

Вызовы энергетической безопасности	Угрозы, способные возникнуть из вызовов
- ВнешЭВ8г) — изменение международного нормативно-правового регулирования в сфере энергетики и условий функционирования мировых энергетических рынков, усиление позиций потребителей; - ВнешЭВ8д) — рост производства сжиженного природного газа и его доли на мировых энергетических рынках, формирование глобального рынка природного газа; - ВнешЭВ8е) — увеличение доли возобновляемых источников энергии в мировом топливно-энергетическом балансе	- ВнешЭВ-У8в) — угрозы, связанные с увеличением мировой ресурсной базы углеводородного сырья, усилением конкуренции экспортеров энергоресурсов, в том числе в связи с появлением новых экспортеров; - ВнешЭВ-У8г) — угрозы, связанные с изменением международного нормативно-правового регулирования в сфере энергетики и условий функционирования мировых энергетических рынков, усилением позиций потребителей; - ВнешЭВ-У8д) — угрозы, связанные с ростом производства сжиженного природного газа и его доли на мировых энергетических рынках, формированием глобального рынка природного газа; - ВнешЭВ-У8е) — угрозы, связанные с увеличением доли возобновляемых источников энергии в мировом топливно-энергетическом балансе
Внешнеполитические вызовы (согласно п. 9 Доктрины): - ВнешПВ9 — наращивание международных усилий по реализации климатической политики и ускоренному переходу к «зеленой экономике»	Угрозы, способные возникнуть из внешнеполитических вызовов: - ВнешПВ-У9 — угрозы, связанные с наращиванием международных усилий по реализации климатической политики и ускоренному переходу к «зеленой экономике»
Внутренние вызовы (согласно п. 15 Доктрины): - ВнВ15а) — переход РФ к новой модели социально-экономического развития, предполагающей структурную трансформацию экономики, сбалансированное пространственное и региональное развитие, модернизацию основных производственных фондов организаций, существенное повышение производительности труда и эффективности экономической деятельности; - ВнВ15б) — демографическая ситуация в РФ (медленный рост численности населения, увеличение в нем доли граждан старшего поколения, сокращение численности трудоспособного населения, внутренняя и внешняя миграция), влияющая как на перспективы внутреннего спроса на продукцию и услуги организаций ТЭК, так и на обеспеченность этих организаций трудовыми ресурсами	Угрозы, способные возникнуть из внутренних вызовов: - ВнВ-У15а) — угрозы, связанные с переходом РФ к новой модели социально-экономического развития, предполагающей структурную трансформацию экономики, сбалансированное пространственное и региональное развитие, модернизацией основных производственных фондов организаций, существенным повышением производительности труда и эффективности экономической деятельности; - ВнВ-У15б) — угрозы, связанные с демографической ситуацией в РФ (медленным ростом численности населения, увеличением в нем доли граждан старшего поколения, сокращением численности трудоспособного населения, внутренней и внешней миграцией), влияющие как на перспективы внутреннего спроса на продукцию и услуги организаций ТЭК, так и на обеспеченность этих организаций трудовыми ресурсами
Трансграничные вызовы (согласно п. 18 Доктрины): - ТрансВ18 — развитие и распространение прорывных технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической энергии, накопителей энергии, добычи углеводородного сырья из трудноизвлекаемых запасов, цифровых и интеллектуальных технологий, энергосберегающих и энергоэффективных технологий на транспорте, в строительстве, жилищно-коммунальном хозяйстве и промышленности	Угрозы, способные возникнуть из трансграничных вызовов: - ТрансВ-У18 — угрозы, связанные с развитием и распространением прорывных технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической энергии, накопителей энергии, добычи углеводородного сырья из трудноизвлекаемых запасов, цифровых и интеллектуальных технологий, энергосберегающих и энергоэффективных технологий на транспорте, в строительстве, жилищно-коммунальном хозяйстве и промышленности

Таблица Г.3 — Характеристика рисков, связанных с разнородными угрозами, и последствий от возможной реализации угроз

Угрозы энергетической безопасности	Риски в области энергетической безопасности
Внешнеэкономические, внешнеполитические и военно-политические угрозы (согласно пп. 8, 9, 11, 13 Доктрины): - угрозы от ВнешЭВ-У8а) до ВнешЭВ-У8е), способные возникнуть из внешнеэкономических вызовов; - угрозы ВнешПВ-У9, способные возникнуть из внешнеполитических вызовов; - ВнешЭУ11а) — сокращение традиционных для РФ внешних энергетических рынков и трудности, связанные с выходом на новые энергетические рынки; - ВнешЭУ11б) — использование иностранными государствами договорно-правовых, международно-правовых и финансовых механизмов в целях нанесения ущерба топливно-энергетическому комплексу РФ и ее экономике в целом; - ВнешЭУ11в) — дискриминация российских организаций ТЭК на мировых энергетических рынках путем изменения международного нормативно-правового регулирования в сфере энергетики, в том числе под предлогом реализации климатической и экологической политики или диверсификации источников импорта энергоресурсов; - ВнешЭУ11г) — незаконный отбор экспортируемых Россией энергоресурсов при их транспортировке по территориям иностранных государств; - ВоенПУ13а) — резкое обострение военно-политической обстановки (межгосударственных отношений) и создание условий для применения военной силы; - ВоенПУ13б) — возникновение и эскалация на территориях государств, сопредельных с Российской Федерацией и ее союзниками, или в других регионах мира вооруженных конфликтов, угрожающих добыче, транспортировке или потреблению российских энергоресурсов, а также ограничивающих возможность использования российских технологий и оказания российскими организациями услуг в сфере энергетики	Риски, связанные с внешними вызовами и угрозами (согласно п. 14 Доктрины): - Р14а) — риск недостаточных темпов реагирования российских организаций ТЭК на тенденции в мировой энергетике, в том числе в части, касающейся освоения новых технологий и коммерческого использования запасов углеводородного сырья; - Р14б) — риск недостаточной эффективности механизмов предупреждения дискриминации российских организаций ТЭК со стороны иностранных государств и их объединений, а также механизмов противодействия такой дискриминации; - Р14в) — недостаточная готовность организаций ТЭК к функционированию в случае реализации военно-политических угроз; - Р14г) — принятие неверных долгосрочных инвестиционных решений в условиях высокой неопределенности мировых энергетических рынков
Внутренние угрозы (согласно пп. 15,16 Доктрины): - угрозы ВнВ-У15а) и ВнВ-У15б), способные возникнуть из внутренних вызовов; - ВнУ16а) — несоответствие возможностей ТЭК потребностям социально-экономического развития РФ (энергетический дефицит или избыток энергетических мощностей и инфраструктуры ТЭК); - ВнУ16б) — снижение качества минерально-сырьевой базы ТЭК (истощение действующих месторождений, уменьшение размеров и снижение качества открываемых месторождений); - ВнУ16в) — недостаточная обеспеченность организаций ТЭК трудовыми ресурсами, в особенности высококвалифицированными кадрами;	Риски, связанные с внутренними вызовами и угрозами (согласно п. 17 Доктрины): - Р17а) — риск несогласованного развития отраслей ТЭК и видов деятельности в сфере энергетики, включая экспорт продукции и услуг организаций ТЭК, в условиях ограниченного государственного контроля и регулирования; - Р17б) — риск отсутствия в долгосрочной перспективе определенности относительно спроса на продукцию и услуги организаций ТЭК в субъектах РФ; - Р17в) — риск низкой эффективности осуществляемых субъектами энергетической безопасности мер по поддержанию финансовой устойчивости организаций ТЭК при наступлении неблагоприятных условий,

Продолжение таблицы Г.3

Угрозы энергетической безопасности	Риски в области энергетической безопасности
- ВнУ16г) — рост количества преступлений и правонарушений в сфере энергетики (хищения, коррупция, производство и продажа контрафактной продукции, неплатежи); - ВнУ16д) — рост количества нарушений в сфере трудовых отношений в организациях ТЭК, жилищно-коммунального хозяйства и транспорта, в том числе нарушений требований охраны труда, а также случаев проведения незаконных забастовок	таких как рост неплатежей за поставленные организациями ТЭК энергоресурсы и оказанные ими услуги, увеличение транспортных расходов и капитальных затрат таких организаций при освоении нефтегазовых месторождений, находящихся в удаленных местностях, усложнение компонентного состава нефтегазовых месторождений; - Р17г) — риск чрезмерной финансовой нагрузки на организации ТЭК в результате увеличения размеров налоговых, таможенных и иных платежей; - Р17д) — риск избыточности требований, касающихся обеспечения экологической безопасности при осуществлении деятельности в отраслях ТЭК, рост затрат организаций ТЭК на обеспечение выполнения таких требований; - Р17е) — риск необоснованной монополизации в отраслях ТЭК и неравных условий конкуренции в конкурентных видах деятельности в сфере энергетики; - Р17ж) — риск высокого уровня износа основных производственных фондов организаций ТЭК, низкой эффективности использования и недостаточных темпов обновления этих фондов; - Р17з) — риск нерационального потребления энергоресурсов; - Р17и) — риск недостаточных темпов реагирования системы профессионального образования на изменение потребности организаций ТЭК в квалифицированных кадрах
Трансграничные угрозы (согласно пп. 18, 19 Доктрины): - угрозы ТрансВ-У18, способные возникнуть из трансграничных вызовов; - ТрансУ19а) — террористическая и диверсионная деятельность, наносящая ущерб инфраструктуре и объектам ТЭК; - ТрансУ19б) — противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов ТЭК; - ТрансУ19в) — неблагоприятные и опасные природные явления, изменения окружающей среды, приводящие к нарушению нормального функционирования и разрушению инфраструктуры и объектов ТЭК	Риски, связанные с трансграничными вызовами и угрозами (согласно п. 20 Доктрины): - Р20а) — несоответствие технологического уровня российских организаций ТЭК современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков; - Р20б) — недостаточное развитие нормативно-правовой базы, сдерживающее внедрение инновационных технологий, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической энергии и цифровых технологий в сфере энергетики; - Р20в) — недостаточная инновационная активность организаций ТЭК и организаций, осуществляющих деятельность в смежных отраслях экономики, ориентация таких организаций на импорт технологий вместо развития отечественного научно-технологического потенциала; - Р20г) — недостаточные темпы разработки и внедрения новых средств антитеррористической защиты инфраструктуры и объектов ТЭК; - Р20д) — недостаточный уровень защищенности инфраструктуры и объектов ТЭК от актов незаконного вмешательства и опасных природных явлений

Окончание таблицы Г.3

Угрозы энергетической безопасности	Риски в области энергетической безопасности
Последствиями реализации угроз энергетической безопасности (согласно п. 21 Доктрины): - Посл21а) — причинение вреда жизни и здоровью граждан; - Посл21б) — нарушение нормального функционирования организаций, в том числе организаций ТЭК, и отраслей экономики РФ; - Посл21в) — увеличение расходов потребителей на организацию альтернативных способов топливо- и энергоснабжения и на создание запасов (резервов) энергоресурсов; - Посл21г) — рост цен (тарифов) на продукцию организаций ТЭК и услуги в сфере энергетики; - Посл21д) — снижение финансовой устойчивости и прекращение деятельности организаций ТЭК; - Посл21е) — уменьшение объема инвестиций в отрасли ТЭК; - Посл21ж) — уменьшение налоговых, таможенных и иных платежей в бюджеты бюджетной системы РФ со стороны организаций ТЭК; - Посл21з) — необходимость выделения дополнительных бюджетных ассигнований на ликвидацию последствий реализации угроз энергетической безопасности	

Для поддержки принятия решений в СУР применимы следующие критерии выработки рациональных упреждающих мер противодействия угрозам (критерии 2-го типа), действующие в условиях внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8–21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24—29 Доктрины) — см. рисунок Г.2:

- критерий КВ1 — критерий удержания интегрального и/или частных рисков в допустимых пределах в течение задаваемого прогнозного периода времени при ограничениях на эксплуатационные условия и ресурсы;



Рисунок Г.2 — Применимые критерии для решения задач выработки рациональных упреждающих мер

- критерий КВ2 — критерий минимизации затрат при ограничениях на допустимый уровень интегрального и/или частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы;
- критерий КВ3 — критерий минимизации интегрального риска при ограничениях на допустимый уровень частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы.

При этом под частными рисками в области энергетической безопасности понимаются (см. таблицы Г.2 и Г.3):
- риски, связанные с внешними вызовами и угрозами энергетической безопасности согласно п. 14 Доктрины, обозначаемые от Р14а) до Р14г);
- риски, связанные с внутренними вызовами и угрозами энергетической безопасности согласно п. 17 Доктрины, обозначаемые от Р17а) до Р17и);
- риски, связанные с трансграничным вызовами и угрозами энергетической безопасности согласно п. 20 Доктрины, обозначаемые от Р20а) до Р20д).

Под интегральным риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба, характеризующее степень отрицательного влияния на состояние энергетической безопасности РФ от реализации всего множества внешнеэкономических, внешнеполитических, военно-политических, внутренних и трансграничных угроз в области энергетической безопасности с учетом возможных последствий.

Примечание — Выполнение требований по защите информации реализуется путем достижения цели Доктрины с условным номером 22к), связанной с обеспечением защищенности критической информационной инфраструктуры объектов ТЭК [27].

По результатам решения задач анализа и выработки рациональных упреждающих мер формируют кратко-, средне- и/или долгосрочные планы по реализации комплекса мер реагирования на невыполнение критичных ограничений на эксплуатационные условия и ресурсы и на недопустимые риски (см. рисунки Г.1 и Г.2).

Планы формируют с привязкой к скоротечности реализации угроз и размеру соответствующего риска, рассчитываемого в динамике изменения состояния уровня энергетической безопасности. Например:

к 1-й группе могут быть отнесены краткосрочные планы по реализации комплекса мер, которые надлежит принять в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода от нескольких недель до полугода;

ко 2-й группе могут быть отнесены среднесрочные планы по реализации комплекса мер, которые надлежит принять в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода от полугода до 3-х лет, что соизмеримо с планированием бюджета РФ на 3 года;

к 3-й группе могут быть отнесены долгосрочные планы по реализации комплекса мер в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода более 3-х лет.

При этом основные направления деятельности по обеспечению энергетической безопасности определены п.24 Доктрины (далее по тексту обозначены от Д24а) до Д24д)). Решаемые по этим направлениям задачи, которые могут находить свое отражение в кратко-, средне- и долгосрочных планах, определены в пп. 25—29 Доктрины (см. таблицу Г.4).

Таблица Г.4 — Задачи для отражения в кратко-, средне- и долгосрочных планах

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
НД24а) — совершенствование государственного управления в области обеспечения энергетической безопасности	- НД24а) — З25а) — совершенствование нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики; - НД24а) — З25б) — создание системы управления рисками в области энергетической безопасности, обеспечение ее взаимодействия с государственными информационными системами, системами мониторинга и прогнозирования чрезвычайных ситуаций на объектах ТЭК, иными системами управления рисками, используемыми субъектами энергетической безопасности; - НД24а) — З25в) — обеспечение стабильности налоговой политики и нормативно-правового регулирования в сфере энергетики, способствующей оптимизации финансовой нагрузки на организации ТЭК и привлечению в них инвестиций; - НД24а) — З25г) — долгосрочное и сбалансированное регулирование цен (тарифов) на товары и услуги субъектов естественных монополий и субъектов, осуществляющих регулируемые виды деятельности, совершенствование ценовой политики в сфере энергетики на внутреннем рынке и планомерный переход к рыночным механизмам ценообразования в этой сфере с учетом социальной ответственности организаций ТЭК;

Продолжение таблицы Г.4

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
	- НД24а) — 325д) — развитие конкуренции в отраслях ТЭК на внутреннем рынке и исключение не отвечающей экономическим интересам Российской Федерации конкуренции между различными видами российских энергоресурсов на мировых энергетических рынках; - НД24а) — 325е) — профилактика и пресечение преступных и противоправных действий в сфере энергетики, в том числе нецелевого использования и хищения бюджетных средств, неплатежей, борьба с коррупцией, теневой экономикой, производством и продажей контрафактной продукции; - НД24а) — 325ж) — пресечение деятельности, осуществляемой специальными службами и организациями иностранных государств, террористическими и экстремистскими организациями, направленной на нанесение ущерба инфраструктуре и объектам ТЭК; - НД24а) — 325з) — осуществление федерального государственного контроля (надзора) за обеспечением безопасности объектов ТЭК, защита объектов ТЭК (в том числе объектов критической информационной инфраструктуры) от совершения актов незаконного вмешательства; - НД24а) — 325и) — внедрение новой модели государственного регулирования в области промышленной безопасности с учетом степени риска возникновения аварий и масштаба их возможных последствий; - НД24а) — 325к) — повышение эффективности федерального государственного надзора в области промышленной безопасности в части, касающейся инфраструктуры и объектов ТЭК, сокращение количества бесхозяйных объектов и совершенствование правовых механизмов привлечения к ответственности за нарушение требований промышленной безопасности; - НД24а) — 325л) — обеспечение безопасных условий труда работников организаций ТЭК, развитие системы управления охраной труда и предупреждения производственного травматизма, совершенствование механизмов государственного контроля (надзора) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права; - НД24а) — 325м) — обеспечение социальной защиты высвобождаемых работников градообразующих организаций угольной промышленности и ликвидация последствий ведения горных работ;
НД24б) — поддержание минерально-сырьевой базы ТЭК и основных производственных фондов организаций ТЭК на уровне, необходимом для обеспечения энергетической безопасности	- НД24а) — 325н) — стимулирование энергосбережения и повышения энергетической эффективности экономики; - НД24б) — 326а) — обеспечение воспроизводства минерально-сырьевой базы ТЭК, повышение эффективности недропользования; - НД24б) — 326б) — обеспечение безопасности при использовании атомной энергии; - НД24б) — 326в) — снижение уязвимости, обеспечение управляемости и живучести инфраструктуры и объектов ТЭК, включая резервирование их мощностей и создание запасов топлива, в том числе для обеспечения его поставок в периоды пикового потребления, в условиях чрезвычайных ситуаций, в период мобилизации и в военное время; - НД24б) — 326г) — поддержание на необходимом уровне запасов продукции организаций ТЭК в государственном материальном резерве; - НД24б) — 326д) — проведение комплексной модернизации и оптимизации основных производственных фондов организаций ТЭК с использованием преимущественно отечественных инновационных, энергоэффективных и экологически безопасных технологий и оборудования, изготовленного на территории Российской Федерации, подготовка необходимых для этого кадров; - НД24б) — 326е) — сбалансированное развитие локальных и интегрируемых в Единую энергетическую систему России распределенных источников энергоснабжения, формирование с их участием локальных интеллектуальных энергетических систем; - НД24б) — 326ж) — уменьшение отрицательного воздействия хозяйственной деятельности организаций ТЭК на окружающую среду

Окончание таблицы Г.4

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
НД24в) — совершенствование территориально-производственной структуры ТЭК с учетом необходимости укрепления единства экономического пространства Российской Федерации	- НД24в) — 327а) — развитие инфраструктуры и объектов ТЭК Восточной Сибири, Арктической зоны Российской Федерации, Дальнего Востока, Северного Кавказа, Крыма и Калининградской области; - НД24в) — 327б) — поддержание технологического единства, надежности, управляемости, непрерывности и безопасности работы Единой системы газоснабжения, Единой энергетической системы России и системы магистральных трубопроводов для транспортировки нефти и нефтепродуктов; - НД24в) — 327в) — развитие внутреннего рынка сжиженного природного газа в целях обеспечения энергетической безопасности территорий, удаленных от Единой системы газоснабжения; - НД24в) — 327г) — обеспечение экономически эффективного сочетания использования систем централизованного электро- и теплоснабжения с развитием распределенной генерации электрической энергии и интеллектуализацией энергетических систем, а также с использованием местных ресурсов, в том числе возобновляемых источников энергии
НД24г) — обеспечение международно-правовой защиты интересов российских организаций ТЭК и энергомашиностроения, поддержка экспорта их продукции, технологий и услуг	- НД24г) — 328а) — развитие интеграционных связей в рамках Евразийского экономического союза и Содружества Независимых Государств, углубление партнерства в сфере энергетики по линии объединения БРИКС, Шанхайской организации сотрудничества, развитие сотрудничества с иностранными государствами в рамках Форума стран — экспортеров газа, с Организацией стран — экспортеров нефти и другими международными организациями; - НД24г) — 328б) — противодействие дискриминации на мировых энергетических рынках российских организаций ТЭК, осуществляющих экспорт продукции, технологий и услуг и участвующих в реализации международных проектов; - НД24г) — 328в) — совершенствование внешнеполитических инструментов и механизмов взаимодействия с основными профильными международными организациями и участниками мировых энергетических рынков в целях обеспечения устойчивого функционирования этих рынков; - НД24г) — 328г) — содействие осуществляемой на равноправной основе международной научно-технологической кооперации, освоению передовых иностранных технологий, стандартов и практик в сфере энергетики
НД24д) — обеспечение технологической независимости ТЭК и повышение его конкурентоспособности	- НД24д) — 329а) — планомерное осуществление импортозамещения в критически важных для устойчивого функционирования ТЭК видах деятельности, в том числе локализация производства иностранного оборудования или создание его отечественных аналогов, разработка технологий (в том числе информационно-телекоммуникационных) и программного обеспечения; - НД24д) — 329б) — развитие отечественного научно-технологического потенциала, создание и освоение передовых технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, наращивание производства на территории Российской Федерации конкурентоспособного основного и вспомогательного оборудования, создание центров компетенций; - НД24д) — 329в) — предотвращение критического отставания Российской Федерации в развитии цифровых и интеллектуальных технологий в сфере энергетики, снижение уязвимости объектов критической информационной инфраструктуры ТЭК; - НД24д) — 329г) — развитие компетенций во всех видах деятельности, критически важных для устойчивого функционирования ТЭК; - НД24д) — 329д) — содействие развитию российского энергомашиностроения и приборостроения, российской электротехнической промышленности; - НД24д) — 329е) — расширение участия организаций ТЭК в развитии системы профессионального образования и дополнительного профессионального образования в сфере энергетики

Перечисленные в таблицах Г.2, Г.3, Г.4 угрозы, риски и задачи представляют собой составные элементы СУР и элементы различных моделируемых систем, изучаемых при решении задач системного анализа в интересах обеспечения энергетической безопасности в РФ.

Г.8.4 Ниже приведены возможные способы по декомпозиции и интеграции моделируемых систем при решении задач системного анализа для различных мета-уровней (например, на уровне РФ в целом, федерального округа, макрорегиона РФ или отдельно взятого субъекта энергетической безопасности).

Г.8.4.1 Способ 1. Мониторинг состояния энергетической безопасности ориентирован по своей сути на систематический сбор и анализ информации от различных источников, связанных с энергетикой (например, от энергетического оборудования). Дополнительно из других источников может быть использована общедоступная информация по политическим, экономическим, научно-технологическим, социальным аспектам, а также по принятому регламенту функционирования объектов ТЭК. Тем самым для каждого мета-уровня обеспечен сбор информации, способствующей объективной характеристике приемлемости или неприемлемости состояния энергетической безопасности по тому или иному показателю (см. способ 4 в Г.8.4.4).

Г.8.4.2 Способ 2. В качестве логической основы системного понимания структурно сложных моделируемых систем применимы «логические деревья», имеющие корень дерева (0-й ярус) и связанные с корнем вершины последующих ярусов (1-го, 2-го и т.д.), характеризующие различные сущности. Последний ярус представляет собой характеристики угроз для моделирования, определяемые по используемым исходным данным. Тем самым обеспечена двунаправленная прослеживаемость цепочки логических умозаключений от корня к конкретной вершине и обратно. А при установлении взаимосвязей разнородных вершин одного яруса и логической интерпретации этих взаимосвязей возможна логическая интерпретация результатов решения задач системного анализа и выработки упреждающих мер применительно ко всему «логическому дереву» в целом. Например, для макрорегиона, рассматриваемого в качестве моделируемой системы, корнем дерева может выступать сам макрорегион (0-й ярус), а в качестве вершин 1-го яруса — субъекты энергетической безопасности этого региона.

Для этих двух уровней логическая интерпретация может быть такова: энергетическая безопасность макрорегиона обеспечена, если обеспечена энергетическая безопасность каждого из субъектов энергетической безопасности этого региона. В основу такого логического описания архитектуры «логического дерева» положены базовые принципы ГОСТ Р 57100.

Г.8.4.3 Способ 3. Используя способы 1 и 2, с учетом основных направлений деятельности по обеспечению энергетической безопасности «логическое дерево» применительно к конкретному федеральному округу может быть сформировано следующим образом. В качестве корня дерева (0-й ярус) выступает сам федеральный округ, а характеристики угроз, используемые в качестве исходных данных при моделировании и расчетах критериев, образуют вершины последнего яруса дерева. Эти последние вершины могут быть представлены с помощью универсальной вспомогательной модели показателя (см. способ 4 в Г.8.4.4).

Применительно к 0-му ярусу — корню (т. е. применительно к рассматриваемому федеральному округу) выбирают соответствующие цели 22а) — 22о) Доктрины. Они образуют 1-й ярус дерева, т. е. каждая цель 22а) — 22о) Доктрины — это вершина 1-го яруса. Всего для условно *i*-го федерального округа РФ максимально может быть 14 вершин 1-го яруса: *i*.1-я вершина обозначена 22а), *i*.14-я вершина — обозначена 22о). Для описания связи «цели — направления деятельности — решаемые задачи — риски — угрозы — характеристики угроз» в качестве вершин 2-го яруса могут рассматриваться направления деятельности для достижения цели, 3-го яруса — решаемые задачи в рамках направления деятельности, на 4-м ярусе — риски для достижения целей путем решения конкретных задач, на 5-м ярусе — угрозы, определяющие эти риски, на 6-м ярусе — характеристики угроз для моделирования.

Например, каждое направление по п.24а) — 24д) Доктрины образует вершину 2-го яруса, всего — 5 вершин 2-го яруса. Так, на рисунке Г.3 от *i*.2-й вершины 1-го яруса идут ветви к вершинам 2-го яруса, тогда соответствующие вершины 2-го яруса обозначаются от 22б) — НД24а) до 22б) — НД24д), а для *i*.12-й вершины 1-го яруса — соответственно от 22м) — НД24а) до 22м) — НД24д).

Решаемые задачи для каждого из направлений деятельности образуют 3-й ярус дерева, т. е. каждая задача по пп. 25—29 Доктрины — это вершины 3-го яруса. Таким образом, для направления деятельности 24а) Доктрины может быть до 13 вершин 3-го яруса. На ветвях от первой вершины 2-го яруса 22а) — НД24а) (такое обозначение для вершины 2-го яруса означает цель, связанную с воспроизводством минерально-сырьевой базы ТЭК согласно п. 22а) Доктрины и направление деятельности «совершенствование государственного управления в области обеспечения энергетической безопасности» согласно п. 24а) Доктрины) образуются вершины 3-го яруса. В частности, первая вершина будет означать первую решаемую задачу – «а)совершенствование нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики» согласно п. 25а) Доктрины, эта вершина будет обозначаться 22а) — НД24а) — 325а), а 13-я вершина 3-го яруса, относящаяся к задаче «н) стимулирование энергосбережения и повышения энергетической эффективности экономики» по п. 25н) Доктрины будет обозначаться 22а) — НД24а) — 325н). Для 5-го направления деятельности 24д) Доктрины всего будет до 6 вершин 3-го яруса. Тогда для этого направления деятельности 1-я вершина яруса обозначается 22а) — НД24д) — 329а), а 6-я вершина, относящаяся к задаче по п. 29е) Доктрины, будет обозначаться 22а) — НД24д) — 329е).

Таким образом, способ 3 описывает «логические деревья», образуемые из вербального описания области приложения СУР для последующего понимания результатов применения структурно сложных моделируемых систем.

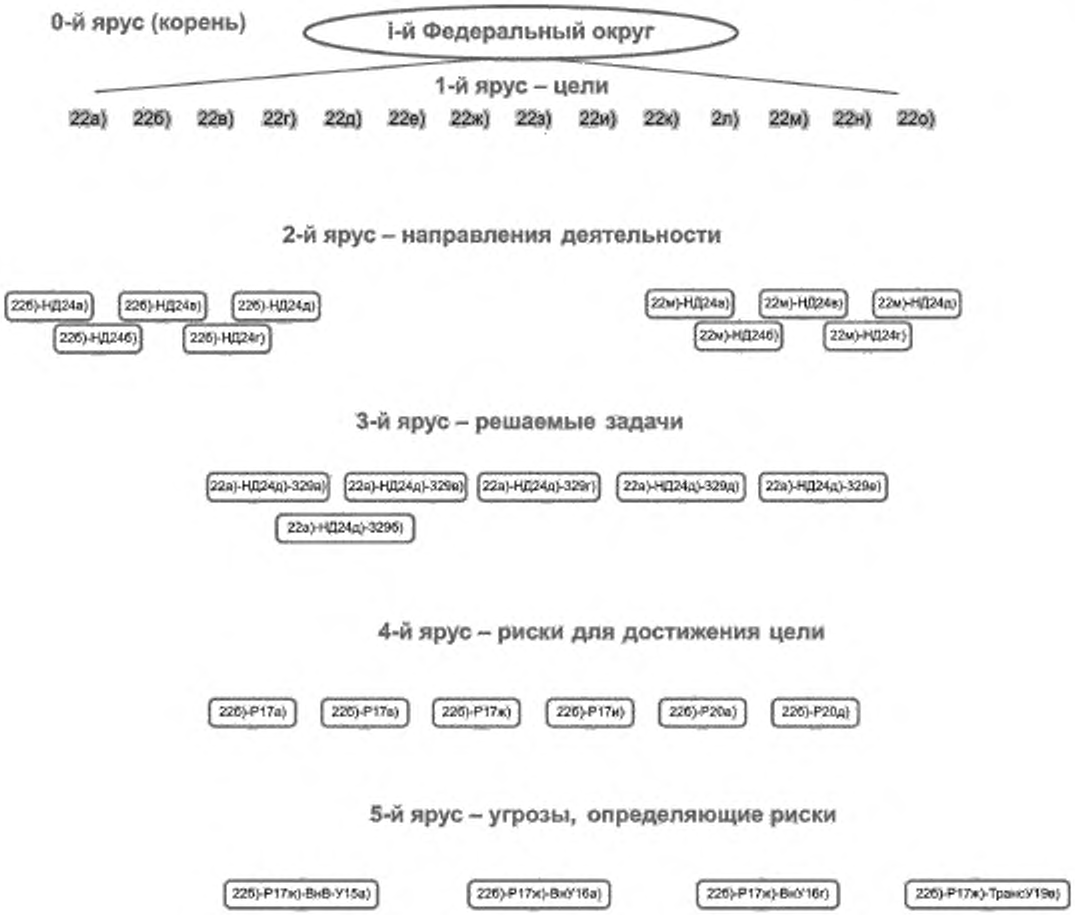


Рисунок Г.3 — «Логическое дерево» для описания связи «цели — направления деятельности — решаемые задачи — риски — угрозы — характеристики угроз»

Г.8.4.4 Способ 4. Для достижения поставленных целей Доктрины, осуществления конкретного направления деятельности и решения каждой из задач по обеспечению энергетической безопасности исходят из того, что в любой момент времени у лиц, принимающих решение, должно быть формальное представление о том, какое состояние энергетической безопасности «приемлемо», а какое «неприемлемо» и требует управляющей реакции для улучшения. Достигнутый уровень состояния энергетической безопасности оценивают различными показателями. Т. е. в каждый отчетный момент времени по каждому из критичных показателей (или по их совокупности) можно с однозначной уверенностью определить, что его (их) значения находятся в зоне, которая может быть охарактеризована как «Приемлемое» состояние или состояние «Приемлемое с отклонением» (когда требуются определенные организационные или обычные технические усилия по улучшению значения показателя) или как «Неприемлемое» состояние (когда требуются кардинальные решения по восстановлению условий и/или ресурсов, которые в существующем виде уже не обеспечивают или в ближайшее время при бездействии не будут гарантировать требуемого уровня энергетической безопасности) (см. рисунок Г.4). Состояния «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» — это элементарные состояния, в которые может переходить во времени каждый из показателей.

Примечание — Способ 4 также применим для случая, когда в качестве критичного показателя выступает неколичественная оценка состояния с градациями «Приемлемое», «Приемлемое с отклонением», «Неприемлемое».

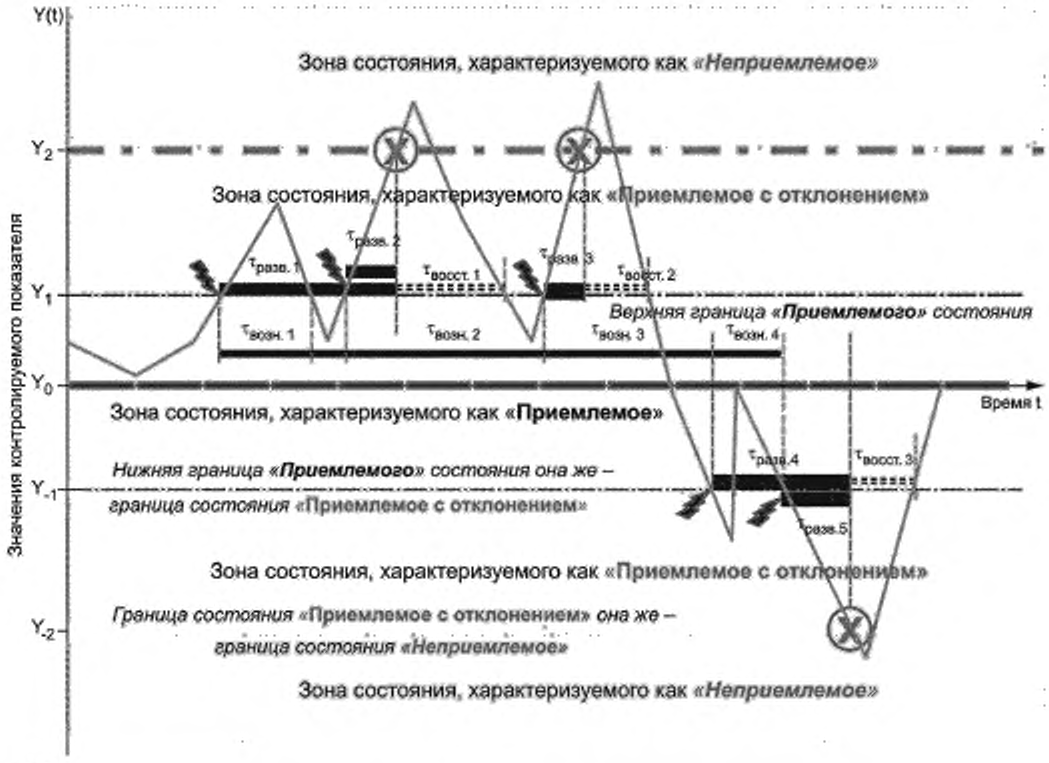


Рисунок Г.4 — Элементарные состояния контролируемого показателя во времени и временные характеристики для прогнозирования рисков

Используя способ 4, разнородные критичные показатели могут быть сведены к универсальной вспомогательной модели показателя (УВМП). В качестве исходных данных УВМП использует только показатели, характеризуемые временем, частотой и возможным ущербом для описания состояния энергетической безопасности.

В общем случае для характеристики каждого показателя на нижнем ярусе «логического дерева», включая УВМП, мониторируемые данные используются для формирования таких значений исходных данных (см. модели приложения В), как частота возникновения источника угроз (σ), среднее время развития угроз с момента возникновения источника угроз до нарушения нормальных условий (β) и среднее время восстановления нарушаемой целостности ($T_{восст}$), например, приемлемых условий и/или ресурсов, необходимых для обеспечения энергобезопасности.

Примечание — Под приемлемыми условиями и/или ресурсами системы понимается такое ее состояние (характеризуемое этими условиями и ресурсами), при котором обеспечивается достижение целей функционирования системы. Такое состояние называют состоянием целостности системы.

Так, согласно рисунку Г.4 частота возникновения источника угроз для моделируемой системы рассчитывается по формуле

$$\sigma = 1/[(\tau_{возн.1} + \tau_{возн.2} + \tau_{возн.3} + \tau_{возн.4})/4],$$

среднее время развития угроз с момента возникновения источника угроз до нарушения нормальных условий функционирования моделируемой системы рассчитывается по формуле

$$\beta = (\tau_{разв.1} + \tau_{разв.2} + \tau_{разв.3} + \tau_{разв.4} + \tau_{разв.5})/5,$$

среднее время восстановления нарушаемой целостности моделируемой системы рассчитывается по формуле

$$T_{восст} = (\tau_{восст.1} + \tau_{восст.2} + \tau_{восст.3})/3,$$

где $\tau_{возн.i}$ — i-й интервал времени между возникновениями источника угроз;

$\tau_{разв.j}$ — j-й интервал времени развития угроз с момента возникновения источника угроз до нарушения нормальных условий;

$\tau_{восст.m}$ — m-й интервал времени восстановления нарушаемой целостности.

Значения σ, β, $T_{восст}$, получаемые по результатам анализа данных мониторинга (или их пересчета на уровне УВМП), являются исходными данными для последующего формального описания моделируемой системы с учетом возможности прогнозирования динамики разнородных событий. Роль в УВМП каждого из учитываемых критичных показателей сводится к их весомости в формируемых значениях σ, β, $T_{восст}$ для УВМП.

Таким образом, способ 4 позволяет сформировать унифицированное пространство элементарных состояний — «Приемлемое» (с выделением для упреждения состояния «Приемлемое с отклонением») и «Неприемлемое» для «логического дерева», а также универсальный механизм использования данных мониторинга для формирования исходных данных при прогнозировании рисков в СУР. Используя доступные временные данные регламента и системной диагностики $T_{меж}$ и $T_{диаг}$, в итоге получаются сформированными исходные данные для применения моделей приложения В.

Г.8.5 Результаты моделирования также подлежат интерпретации. Например, в цепочке «цели — направления деятельности — решаемые задачи — риски — угрозы — характеристики угроз» для поддержки принятия решений по выработке рациональных упреждающих мер противодействия угрозам с использованием фрагмента «логического дерева» в части рисков, относящихся к цели 22б), направлению деятельности 22б) — НД24д), решаемой задаче 22а) — НД24д) — 329б) интегральный риск недостижения цели может быть интерпретирован следующим образом (см. рисунок Г.5).

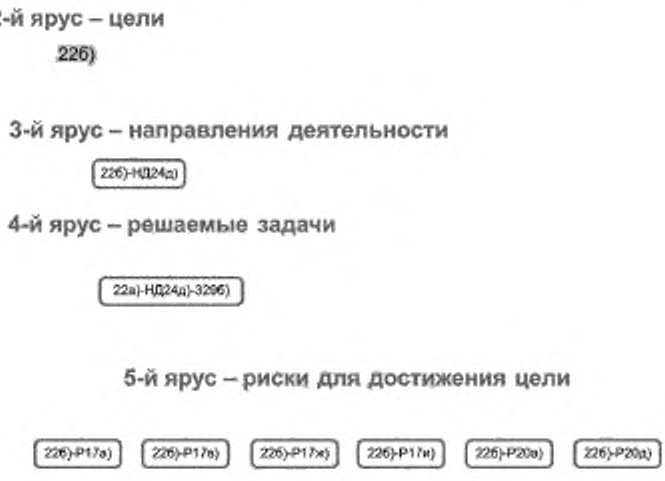


Рисунок Г.5 — Фрагмент, когда интегральный риск на уровне цели определяется составными рисками в рамках направления деятельности и решаемой задачи

Интерпретация: надежное и устойчивое обеспечение российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики в течение задаваемого периода прогноза при решении задачи развития отечественного научно-технологического потенциала, создания и освоения передовых технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, наращивание производства на территории РФ конкурентоспособного основного и вспомогательного оборудования, создание центров компетенций (см. 22а) — НД24д) — 329б)) в рамках направления деятельности по обеспечению технологической

независимости ТЭК и повышения его конкурентоспособности (см. 22б) — НД24д)) окажется в состоянии «Неприемлемое», если в течение этого срока превысят допустимый уровень:

ИЛИ риск несогласованного развития отраслей ТЭК и видов деятельности в сфере энергетики, включая экспорт продукции и услуг организаций ТЭК, в условиях ограниченного государственного контроля и регулирования (см. 22б) — Р17а));

ИЛИ риск низкой эффективности осуществляемых субъектами энергетической безопасности мер по поддержанию финансовой устойчивости организаций ТЭК при наступлении неблагоприятных условий, таких как рост неплатежей за поставленные организациями ТЭК энергоресурсы и оказанные ими услуги, увеличение транспортных расходов и капитальных затрат таких организаций при освоении нефтегазовых месторождений, находящихся в удаленных местностях, усложнение компонентного состава нефтегазовых месторождений (см. 22б) — Р17в));

ИЛИ риск высокого уровня износа основных производственных фондов организаций ТЭК, низкая эффективность использования и недостаточные темпы обновления этих фондов (см. 22б) — Р17ж));

ИЛИ риск недостаточных темпов реагирования системы профессионального образования на изменение потребности организаций ТЭК в квалифицированных кадрах (см. 22б) — Р17и));

ИЛИ риск несоответствия технологического уровня российских организаций ТЭК современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков (см. 22б) — Р20а));

ИЛИ риск недостаточного уровня защищенности инфраструктуры и объектов ТЭК от актов незаконного вмешательства и опасных природных явлений (см. 22б) — Р20д)).

В ином случае по указанной цели, направлению деятельности и решаемой задаче энергетическая безопасность в течение задаваемого периода прогноза будет находиться в состоянии «Приемлемое» или «Приемлемое с отклонением» с непревышением допустимых рисков.

Г.8.6 Далее с использованием положений, методов и моделей приложения В становится возможным осуществление расчетов рисков для сложных структур и учет требований по защите информации. Сбалансированное упреждающее управление процессами возникновения, развития, контроля и нейтрализации возможных угроз осуществляется как результат решения формально постановленных задач системного анализа путем целенаправленного использования моделей и выбранных критериев при соответствующих ограничениях (см. таблицу Г.1).

Для расчетов составных показателей используют модели и методы из таблицы В.1. Так, для расчетов интегрального риска по формуле (В.11) расчет составного показателя $R_{\text{надежн}}(T_{\text{зад}})$, определяющего вероятность нарушения надежности реализации процесса системного анализа в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации, вычисляют по моделям и рекомендациям В.3 и В.4. Расчет составного показателя $R_{\text{наруш}}(T_{\text{зад}})$, определяющего вероятность нарушения требований по защите информации в системе для процесса системного анализа в течение периода прогноза $T_{\text{зад}}$, вычисляют по моделям и рекомендациям В.5. При этом выполнение требований по защите информации анализируют в рамках достижения цели Доктрины с условным номером 22к), связанной с обеспечением защищенности критической информационной инфраструктуры объектов ТЭК. В итоге становится возможным применение формулы (В.11) для расчетов интегрального риска нарушения надежности реализации процесса системного анализа с учетом требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$, для прогнозного периода $T_{\text{зад}}$ в сопоставлении с возможным ущербом (см. В.6).

Г.8.7 Итогом завершения логического преобразования в Г.8.1 — Г.8.6 изначального вербального описания системы (см. [27], [28]) является вид формализации, представленный на рисунках Г.1 — Г.5 в обозначениях, приведенных в таблицах Г.2 — Г.4. Этот вид позволяет осуществить формальные постановки практических задач системного анализа энергетической безопасности (см. таблицу Г.1), используя модели и методы приложения В. Например, с использованием информации, собираемой и обрабатываемой в СУР, могут быть формально поставлены и решены задачи:

- минимизации риска нарушения надежности обеспечения энергетической безопасности макрорегиона РФ или отдельно взятого субъекта энергетической безопасности в ТЭК при ограничениях на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и общие затраты на реализацию планов и при иных ограничениях;

- минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях на допустимый риск надежности обеспечения энергетической безопасности макрорегиона РФ или отдельно взятого субъекта энергетической безопасности в ТЭК, на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и при иных ограничениях;

- комбинации перечисленных выше или иных оптимизационных задач применительно к макрорегиону или отдельно взятому субъекту энергетической безопасности в ТЭК.

Результаты решения этих задач могут быть использованы для обеспечения баланса по критерию «эффективность — стоимость» при кратко-, средне- и/или долгосрочном планировании на уровне макрорегиона РФ или отдельно взятого субъекта энергетической безопасности.

Г.8.8 Для решения формально поставленных задач применяют любые научно обоснованные расчетные методы, позволяющие достигать поставленных целей системного анализа. Многочисленные примеры решения задач системного анализа, связанные с расчетами рисков нарушения реализации конкретного процесса, рисков на-

рушения требований по защите информации и интегральных рисков нарушения реализации системных процессов с учетом требований по защите информации на основе применения моделей приложения В разобраны в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Г.9 Материально-техническое обеспечение

В состав материально-технического обеспечения для прогнозирования рисков входят:

- результаты обследования, концепция создания, технический облик и/или ТЗ на разработку (для создаваемой системы), конструкторская и эксплуатационная документация (для существующей системы), их используют для формирования исходных данных при моделировании;
- модель угроз безопасности информации (ее 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 (их используют для формирования исходных данных при моделировании);
- планы ликвидации нарушений, инцидентов и аварий, связанных с нарушением требований по защите информации, и восстановления целостности системы (их 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 (их используют для формирования исходных данных при моделировании и обоснования усовершенствований в результате решения задач системного анализа);
- программные комплексы, поддерживающие применение математических моделей и методов (их используют для проведения расчетов и поддержки процедур системного анализа).

Г.10 Отчетность

По результатам решения задач системного анализа составляют отчет по ГОСТ 7.32 или по форме, устанавливаемой в организации.

Примечание — Примером практического применения методических указаний может служить ГОСТ Р 58494, в котором положения системного анализа рекомендованы к реализации на уровне функций систем дистанционного контроля промышленной безопасности, обеспечивающих в опасном производстве принятие решений в режиме реального времени.

Приложение Д
(справочное)

Типовые допустимые значения показателей рисков для процесса системного анализа

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, и требования при рисках, свойственных реальной или гипотетичной системе-эталону. При формировании требований системной инженерии необходимо обоснование достижимости целей системы и рассматриваемого процесса системного анализа, 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 самой системы, увеличивает время до ее принятия в эксплуатацию, а также удорожает эксплуатацию системы.

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

Типовые допустимые значения показателей рисков для процесса системного анализа 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 качественной и безопасной реализации 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 системного анализа	Не выше 0,05	Не выше 0,01
Интегральный риск нарушения надежности реализации процесса системного анализа с учетом требований по защите информации	Не выше 0,05	Не выше 0,01

Ссылочные рекомендации по определению допустимых значений показателей рисков, используемых в системном анализе других системных процессов по ГОСТ Р 57193, отражены в таблице Д.2.

Таблица Д.2 — Ссылки для определения допустимых значений рисков в системных процессах

Системный процесс	Ссылки на стандарты для определения допустимых значений рисков при ориентации на обоснование по прецедентному принципу и для системы-эталона
Процессы приобретения и поставки продукции и услуг для системы	ГОСТ Р 59329—2021, приложение Г
Процесс управления моделью жизненного цикла системы	ГОСТ Р 59330—2021, Приложение Г
Процесс управления инфраструктурой системы	ГОСТ Р 59331—2021, Приложение Д
Процесс управления портфелем проектов	ГОСТ Р 59332—2021, Приложение Г
Процесс управления человеческими ресурсами системы	ГОСТ Р 59333—2021, Приложение Д
Процесс управления качеством системы	ГОСТ Р 59334—2021, Приложение Г
Процесс управления знаниями о системе	ГОСТ Р 59335—2021, Приложение Д
Процесс планирования проекта	ГОСТ Р 59336—2021, Приложение Г
Процесс оценки и контроля проекта	ГОСТ Р 59337—2021, Приложение Г
Процесс управления решениями	ГОСТ Р 59338—2021, Приложение Д
Процесс управления рисками для системы	ГОСТ Р 59339—2021, Приложение Г
Процесс управления конфигурацией системы	ГОСТ Р 59340—2021, Приложение Г
Процесс управления информацией системы	ГОСТ Р 59341—2021, Приложение Д
Процесс измерений системы	ГОСТ Р 59342—2021, Приложение Г
Процесс гарантии качества для системы	ГОСТ Р 59343—2021, Приложение Д
Процесс анализа бизнеса или назначения системы	ГОСТ Р 59344—2021, Приложение Г
Процесс определения потребностей и требований заинтересованной стороны для системы	ГОСТ Р 59345—2021, Приложение Д
Процесс определения системных требований	ГОСТ Р 59346—2021, Приложение Е
Процесс определения архитектуры системы	ГОСТ Р 59347—2021, Приложение Д
Процесс определения проекта	ГОСТ Р 59348—2021, Приложение Г
Процесс реализации системы	ГОСТ Р 59350—2021, Приложение Г
Процесс комплексирования системы	ГОСТ Р 59351—2021, Приложение Г
Процесс верификации системы	ГОСТ Р 59352—2021, Приложение Г
Процесс передачи системы	ГОСТ Р 59353—2021, Приложение Г
Процесс аттестации системы	ГОСТ Р 59354—2021, Приложение Г
Процесс функционирования системы	ГОСТ Р 59355—2021, Приложение Д
Процесс сопровождения системы	ГОСТ Р 59356—2021, Приложение Д
Процесс изъятия и списания системы	ГОСТ Р 59357—2021, Приложение Г

Приложение Е
(справочное)

Примерный перечень методик системного анализа

Е.1 Методика прогнозирования риска нарушения требований по защите информации в процессе системного анализа.

Е.2 Методика прогнозирования интегрального риска нарушения надежности реализации процесса системного анализа с учетом требований по защите информации.

Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации.

Е.4 Методики выявления явных и скрытых недостатков процесса системного анализа с использованием прогнозирования рисков.

Е.5 Методики обоснования предупреждающих мер для достижения целей процесса системного анализа и противодействия угрозам нарушения требований по защите информации.

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

Е.7 Методики выявления явных и скрытых угроз нарушения надежности реализации системных процессов (по ГОСТ Р 57193) с использованием прогнозирования рисков.

Е.8 Методики решения задач минимизации интегрального риска нарушения безопасности системы при кратко-, средне- и долгосрочном планировании и ограничениях (на отдельные допустимые риски реализации существенных угроз, на ресурсы, общие затраты и при иных ограничениях), учитывающих специфику системы.

Е.9 Методики решения задач минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях (на интегральный риск нарушения безопасности системы, на отдельные допустимые риски реализации существенных угроз, на ресурсы и при иных ограничениях), учитывающих специфику системы.

Примечания

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

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

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

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

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

[21] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом Федеральной службы по техническому и экспортному контролю Российской Федерации 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 Федеральной службы по техническому и экспортному контролю Российской Федерации 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 Федеральной службы по техническому и экспортному контролю Российской Федерации от 14 марта 2014 г. № 31)

[24] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом Федеральной службы по техническому и экспортному контролю Российской Федерации 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] Доктрина энергетической безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 13 мая 2019 г. № 216)

[28] Энергетическая стратегия Российской Федерации на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 9 июня 2020 г. № 1523-р)

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

Ключевые слова: системная инженерия, защита информации, процесс системного анализа, актив, безопасность, метод, модель, решение, риск, управление

Технический редактор *И.Е Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Урецкого*

Сдано в набор 19.05.2021. Подписано в печать 21.06.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 8,37. Уч.-изд. л. 7,53.

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