ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59345— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ ПОТРЕБНОСТЕЙ И ТРЕБОВАНИЙ ЗАИНТЕРЕСОВАННОЙ СТОРОНЫ ДЛЯ СИСТЕМЫ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 апреля 2021 г. № 331-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны 8
5 Общие требования системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны 9
6 Специальные требования к количественным показателям 11
7 Требования к системному анализу 13
Приложение А (справочное) Пример перечня защищаемых активов 14
Приложение Б (справочное) Пример перечня угроз 15
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 16
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса определения потребностей и требований заинтересованной стороны 25
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса определения потребностей и требований заинтересованной стороны 37
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса определения потребностей и требований заинтересованной стороны 38
Библиография 39

Введение

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

- для процессов соглашения — процессов приобретения и поставки продукции и услуг для системы — по ГОСТ Р 59329;
- для процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;
- для процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления 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 системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи, аттестации, функционирования, сопровождения, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357. Для процесса определения потребностей и требований заинтересованной стороны для системы — по настоящему стандарту.

Стандарт устанавливает основные требования системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны для рассматриваемой системы и специальные требования к используемым количественным показателям.

Для планируемого и реализуемого процесса определения потребностей и требований заинтересованной стороны 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 ОПРЕДЕЛЕНИЯ ПОТРЕБНОСТЕЙ И ТРЕБОВАНИЙ ЗАИНТЕРЕСОВАННОЙ СТОРОНЫ ДЛЯ СИСТЕМЫ

System engineering. Protection of information in stakeholder needs and requirements definition process for system

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа для процесса определения потребностей и требований заинтересованной стороны применительно к вопросам защиты информации в системах различных областей приложения.

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

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

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем и выведении систем из эксплуатации и реализующими процесс определения потребностей и требований заинтересованной стороны, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем — см. примеры систем в [1]—[24].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

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

Издание официальное

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

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

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

ГОСТ Р 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/EEE 42010:2011 Системная и программная инженерия. Описание архитектуры

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

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

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

ГОСТ Р 59332 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 Системная инженерия. Защита информации в процессе управления качеством системы

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р МЭК 61508-4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61508-5 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 61508-6 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

ГОСТ Р МЭК 61508-7 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ГОСТ Р МЭК 62264-1 Интеграция систем управления предприятием. Часть 1. Модели и терминология

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

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 34.003, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 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 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, а также следующие термины с соответствующими определениями:

3.1.1

актив: Что либо, что имеет ценность для организации.

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

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

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.3

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

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

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

[ГОСТ Р 57193—2016, пункт 4.1.42]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.5

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.6

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.7

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

3.1.9 **надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы:** Свойство процесса определения потребностей и требований заинтересованной стороны для системы сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса в заданных условиях его реализации.

3.1.10

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.11

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.12

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

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

[ГОСТ Р 57193—2016, пункт 4.1.50]

3.1.13

поставщик: Организация или лицо, которые вступают в соглашение с приобретающей стороной на поставку продукта или услуги.

Примечания

1 Поставщиком может быть подрядчик, производитель, торговец или продавец.

2 Иногда приобретающая сторона и поставщик являются частью одной и той же организации.

[ГОСТ Р 57193—2016, пункт 4.1.43]

3.1.14

приобретающая сторона: Заинтересованная сторона, которая приобретает или получает продукт или услугу от поставщика.

Примечание — Другими широко используемыми терминами, обозначающими это понятие, являются покупатель, заказчик, владелец, плательщик или внешний/внутренний спонсор.

[ГОСТ Р 57193—2016, пункт 4.1.1]

3.1.15

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

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

3.1.17

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]

3.1.18

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

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

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

3.1.19

требование по защите информации: Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.
[ГОСТ Р 50922—2006, статья 2.9.2]

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

3.1.21

эффективность защиты информации: Степень соответствия результатов защиты информации цели защиты информации.
[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использовано следующее сокращение:

ПО — программное обеспечение;

СДК — система дистанционного контроля (промышленной безопасности опасного производственного объекта);

ТЗ — техническое задание.

4 Основные положения системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны

4.1 Общие положения

Организации используют данный процесс в рамках создания (модернизации, развития), эксплуатации системы и выведении системы из эксплуатации для выявления потребностей заинтересованной стороны и преобразования их в явно сформулированные формализованные требования.

В процессе определения потребностей и требований заинтересованной стороны для системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должно быть обеспечено надежное выполнение процесса.

Для прогнозирования интегрального риска нарушения реализации процесса и обоснования эффективных предупреждающих мер по снижению этого риска или удержанию его в допустимых пределах используют системный анализ процесса с учетом требований по защите информации.

Определение выходных результатов процесса определения потребностей и требований заинтересованной стороны 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/МЭК 15704, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Оценку интегрального риска с учетом требований по защите информации в процессе определения потребностей и требований заинтересованной стороны осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59355. При этом учитывают специфику системы (см., например, [20]—[24]) и организации, применяющей процесс.

4.2 Цели процесса и назначение мер защиты информации

4.2.1 Формирование целей процесса определения потребностей и требований заинтересованной стороны для системы осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики системы.

В общем случае целью процесса является определение требований к системе, выполнение которых должно обеспечить удовлетворение потребностей каждой из заинтересованных сторон в заданной среде применения системы. Сначала в рамках процесса определяют заинтересованные стороны, связанные с системой на протяжении всего жизненного цикла, и их потребности. Далее в рамках процесса выявленные потребности анализируют и преобразуют в совокупность формальных требований, отражающих желаемое поведение системы в среде функционирования. В последующем эти требования служат исходными данными для выполнения процесса определения системных требований, а также для проверки соответствия эксплуатационных возможностей системы потребностям заинтересованных сторон в рамках процессов функционирования и аттестации системы.

4.2.2 Меры защиты информации в процессе определения потребностей и требований заинтересованной стороны для системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [20]—[24] с учетом специфики системы.

4.3 Стадии и этапы жизненного цикла системы

Процесс определения потребностей и требований заинтересованной стороны для системы используется главным образом на стадии замысла, формирования требований, разработки концепции и ТЗ. Уточнение потребностей и требований заинтересованной стороны может понадобиться также на последующих стадиях, в том числе на стадии выведения системы из эксплуатации.

Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом специфики и условий ее функционирования и требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 59329. Процесс определения потребностей и требований заинтересованной стороны для системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости включать в себя другие процессы.

4.4 Основные принципы

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

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе определения потребностей и требований заинтересованной стороны для системы сосредотачивают:

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

5 Общие требования системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы (в качестве которой может выступать система защиты информации), в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований по защите информации формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например, [20]—[24]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

Поскольку элементы процесса определения потребностей и требований заинтересованной стороны могут использоваться на этапах, предваряющих получение и утверждение ТЗ, соответствующие требования по защите информации, применимые к этому процессу, могут быть оговорены в рамках соответствующих соглашений.

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 определения потребностей и требований заинтересованной стороны для системы и поддержке при этом эффективности защиты информации.

Требования системной инженерии по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы включают:

- требования к составам выходных результатов процесса, выполняемых действий и используемых при этом активов, требующих защиты информации;

- требования к определению потенциальных угроз для выходных результатов и выполняемых действий процесса, а также возможных сценариев возникновения и развития этих угроз;

- требования к прогнозированию рисков при планировании и реализации процессов, обоснованию эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

5.3 Состав выходных результатов и выполняемых действий в процессе определения потребностей и требований заинтересованной стороны для системы определяют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики системы.

5.4 Меры защиты информации и действия по защите информации должны охватывать активы, информация которых или о которых необходима для получения выходных результатов и выполнения действий в процессе определения потребностей и требований заинтересованной стороны для системы.

Примечание — В состав активов могут быть включены активы, используемые при определении потребностей и требований для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заинтересованной стороны — например, привлекаемые средства контроля качества поставляемой продукции у поставщика.

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, [20]—[24].

Примеры перечней учитываемых активов и угроз в процессе определения потребностей и требований заинтересованной стороны для системы приведены в приложениях А и Б.

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

Системный анализ процесса осуществляют с использованием методов, моделей и методик (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, [20]—[24].

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

Типовые модели и методы прогнозирования рисков в процессе определения потребностей и требований заинтересованной стороны для системы, методические указания по прогнозированию рисков, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д, Е. Характеристики мер 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 приложении к защищаемым активам, действиям и выходным результатам процесса определения потребностей и требований заинтересованной стороны для системы, к которым предъявлены определенные требования по защите информации, выполняют оценку эффективности защиты информации на основе прогнозирования рисков в условиях возможных угроз.

6.1.2 В общем случае основными выходными результатами процесса определения потребностей и требований заинтересованной стороны для системы являются:

- концепция функционирования (эксплуатации) системы и иные концепции в жизненном цикле системы;
- установленный состав заинтересованных сторон, имеющих интерес к системе на отдельных этапах или на всех этапах ее жизненного цикла;
- выявленные потребности заинтересованных сторон;
- конкретные формализованные требования к системе, отражающие потребности заинтересованных сторон;
- отчеты по системному анализу формализованных требований;
- карта прослеживаемости сформулированных формализованных требований относительно удовлетворения потребностей заинтересованных сторон;
- характеристики и условия использования возможностей системы, критические показатели ее функционирования;
- ограничения для принимаемых системных решений;
- требования к обеспечивающим системам, которые предполагается использовать для удовлетворения выявленных потребностей заинтересованных сторон и выполнения установленных формализованных требований;
- достигнутые соглашения с заинтересованными сторонами о том, что их потребности правильно отражены в сформулированных формализованных требованиях к системе;
- функциональное описание системы, включая границы ее возможностей и взаимодействия;
- меры по обеспечению функционирования в критических условиях;
- материалы в отчеты об обследовании объектов, проведении необходимых научно-исследовательских работ и требования ТЗ.

6.1.3 Для получения выходных результатов процесса определения потребностей и требований заинтересованной стороны для системы в общем случае выполняют следующие основные действия:

- подготовительные действия:
  - определение заинтересованных сторон, имеющих законный интерес к системе в течение ее жизненного цикла,
  - определение стратегии выполнения процесса для установления общего множества согласованных приемлемых требований к системе,
  - анализ необходимости применения обеспечивающих систем или услуг для определения потребностей и требований заинтересованных сторон, планирование их приобретения и применения,
  - получение или приобретение доступа к обеспечивающим системам или услугам (при необходимости их применения);
- определение потребностей заинтересованных сторон:
  - определение контекста использования системы в пределах концепции ее функционирования (эксплуатации) и основных понятий ее жизненного цикла,
  - выявление явных и подразумеваемых потребностей,
  - распределение выявленных потребностей по приоритетам,
  - определение потребностей заинтересованных сторон и их обоснование, ориентированное на достижение целей системы;
- разработку концепции функционирования (эксплуатации) системы и иных концепций в жизненном цикле системы, включая определение сценариев функционирования и порядка взаимодействия пользователей с системой для обеспечения потребностей заинтересованных сторон;
- преобразование потребностей заинтересованных сторон в конкретные формализованные требования, включая:
  - требования к критичным характеристикам, в том числе по гарантиям безопасности, защищенности окружающей среды и здоровья,

- требования, связанные со сценариями, требующими выполнения функций согласно эксплуатационным и иным концепциям в жизненном цикле системы, обеспечения необходимого взаимодействия, ориентации на ограничительные условия и на критичные характеристики качества, безопасности и эффективности системы,

- ограничения для системных решений, вытекающие из существующих соглашений, управленческих и технических решений;

- анализ потребностей и формализованных требований заинтересованных сторон, включая:

- определение критичных показателей функционирования, позволяющих проводить оценку технического уровня и эффективности принимаемых решений,

- доведение результатов анализа до заинтересованных сторон для получения гарантии того, что их потребности учтены и формально выражены корректным образом,

- разрешение проблем в тех случаях, когда обнаружены нарушения в формулировании частных требований или множества требований;

- управление процессом определения потребностей и требований заинтересованных сторон, включая:

- документирование соглашения в части учета потребностей и требований заинтересованных сторон, в т. ч. реализацию обратной связи для подтверждения гарантий того, что потребности заинтересованных сторон корректно выражены в формализованных требованиях,

- обеспечение прослеживаемости потребностей и требований заинтересованных сторон, подлежащих учету в системных требованиях,

- поддержание основных информационных активов, связанных с реализацией рассматриваемого процесса.

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 определения потребностей и требований заинтересованной стороны для системы 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 нарушения эффективности на ранних этапах проявления явных и скрытых угроз, 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 сравнить эффективность применяемых и/или возможных мер в действующей системе защиты информации.

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе определения потребностей и требований заинтересованной стороны для системы используют следующие количественные показатели:

- риск нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы без учета требований по защите информации;

- риск нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы;

- интегральный риск нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации.

6.3.2 Риск нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы без учета требований по защите информации характеризуют соответствующей вероятностью в зависимости от нарушения надежности реализации процесса в сопоставлении с возможным ущербом.

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

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

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессу определения потребностей и требований заинтересованной стороны для системы):

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

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к системному анализу

Требования к системному анализу процесса определения потребностей и требований заинтересованной стороны включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в процессе определения потребностей и требований заинтересованной стороны.

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

При обосновании и формулировании конкретных требований к системному анализу дополнительно руководствуются положениями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы — см., например, [21]—[24].

Примечание — Примеры решения задач системного анализа применительно к рассматриваемому процессу см. в приложении Г, а применительно к другим процессам — в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе определения потребностей и требований заинтересованной стороны для системы может включать (в части, свойственной этому процессу):

- выходные результаты процесса — по 6.1.2;
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации — по [21]—[24];
- договоры и соглашения, связанные с учетом и удовлетворением потребностей и требований заинтересованных сторон;
- финансовые и плановые документы, связанные с удовлетворением формализованных требований заинтересованных сторон, в том числе при эксплуатации системы, проведении работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601, ТЗ — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839, конструкторскую и технологическую документацию (для модернизируемой или применяемой системы) — по ГОСТ 2.102, ГОСТ 2.602, ГОСТ 3.1001, ГОСТ 34.201, ГОСТ Р 2.601 в части учета потребностей и требований заинтересованных сторон;
- персональные данные, базу данных и базу знаний, систему хранения архивов, систему передачи данных и облачные данные организации, связанные с учетом потребностей и требований заинтересованных сторон;
- выходные результаты иных процессов в жизненном цикле системы, связанные с удовлетворением потребностей и требований заинтересованных сторон.

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе определения потребностей и требований заинтересованной стороны для системы может включать (в части, свойственной этому процессу):

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

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе определения потребностей и требований заинтересованной стороны для системы могут применяться любые возможные методы, обеспечивающие приемлемое достижение поставленных целей.

Типовые методы и модели обеспечивают вероятностную оценку следующих показателей согласно 6.3:

- риска нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы без учета требований по защите информации — см. В.3;
- риска нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы — см. В.2;
- интегрального риска нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации — см. В.4.

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

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

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

В.1.4 Для математической формализации используют следующие основные положения:

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

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

В.1.5 Ниже в В.2.1—В.2.2 приведены математические модели для прогнозирования рисков в системе, представляемой в виде «черного ящика». Модель В.2.1 для прогнозирования рисков при отсутствии какого-либо контроля (диагностики) целостности моделируемой системы является частным случаем модели В.2.2 при реализации технологии периодического системного контроля. Модель В.2.1 применима на практике лишь для оценки и сравнения случая полностью бесконтрольного функционирования рассматриваемой системы, например там, где контроль невозможен или нецелесообразен по функциональным, экономическим или временным соображениям, или когда ответственные лица пренебрегают функциями контроля или не реагируют должным образом на результаты системного анализа.

В.1.6 Для моделируемой системы сложной структуры применимы методы, изложенные в В.2.3, включая методы комбинации и повышения адекватности моделей.

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

В.1.8 Изложение моделей в В.2 дано в контексте нарушения требований по защите информации, в В.3 приведены способы прогнозирования риска нарушения надежности реализации рассматриваемого процесса с использованием адаптированных моделей В.2. Методы прогнозирования интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации представлены в В.4. При этом интегральный риск нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации этого процесса без учета требований по защите информации и риска нарушения требований по защите информации в этом процессе.

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

В.1.9 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 событий на временной оси образуют два основных состояния:

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

В результате математического моделирования рассчитывают вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение до 1, 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.

Примечание — Другие возможные подходы для оценки рисков описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356, ГОСТ Р МЭК 61069-1—ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

В.2 Математические модели для прогнозирования риска нарушения требований по защите информации

В.2.1 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 требований по защите информации осуществляется по мере свершившегося нарушения. При функционировании в результате возникновения и развития угроз может произойти нарушение возможностей системы по обеспечению выполнения требований по защите информации. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения требований по защите информации рассматриваемой системы в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны в течение заданного периода прогноза при отсутствии какого-либо контроля.

Модель представляет собой частный случай модели В.2.2, если период между моментами контроля выполнения требований по защите информации в системе больше периода прогноза. Учитывая это, используют формулы (В.1)—(В.3) из В.2.2.

В.2.2 Математическая модель «черного ящика» при реализации технологии периодического системного контроля

В моделируемой системе, представленной в виде «черного ящика», осуществляется периодический контроль (диагностика) выполнения требований по защите информации.

Из-за случайного характера угроз, различных организационных, программно-технических и технологических причин, различного уровня квалификации специалистов, привлекаемых для контроля, неэффективных мер поддержания или восстановления приемлемых условий функционирования системы и в силу иных причин выполнение требований по защите информации в системе может быть нарушено. Такое нарушение способно повлечь за собой негативные последствия с недопустимым ущербом для системы.

В рамках модели развитие событий в системе считается не нарушающим требований по защите информации в течение заданного периода прогноза, если к началу этого периода выполнение требований по защите информации в системе обеспечено 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) выполнения требований по защите информации, но и способы поддержания и/или восстановления возможностей по обеспечению их выполнения при выявлении источников (предпосылок к потенциальному нарушению) или следов активизации угроз (т. е. фактов состоявшегося нарушения). Восстановление целостности моделируемой системы осуществляется лишь в период системного контроля. Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии ненарушения требований по защите информации в системе из-за возможных угроз за период прогноза (т. к. нарушения устраняют за счет предупреждающих действий по результатам очередной системной диагностики состояния моделируемой системы).

За основу анализа принят следующий последовательный алгоритм возникновения и развития потенциальной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться, представляя угрозу для нарушения требований по защите информации. По прошествии периода активизации, свойственного этому источнику угрозы (в общем случае этот период активизации представляет собой случайную величину), наступает виртуальный момент нарушения, интерпретируемый как момент нарушения требований по защите информации с возможными негативными последствиями.

Примечание — Если активизация мгновенная, это считают эквивалентным внезапному отказу в приложении к надежности систем. Возможности системы защиты информации как раз и направлены на использование времени постепенной активизации угроз для своевременного выявления, распознавания и противодействия этим угрозам.

Выполнение требований по защите информации в моделируемой системе считается нарушенным лишь после того, как активизация источника угрозы происходит за период прогноза (т. е. возникает элементарное состояние «Выполнение требований по защите информации в системе нарушено»). При отсутствии нарушений результатом применения очередной системной диагностики является подтверждение возможностей по обеспечению выполнения требований по защите информации, а при наличии нарушений перед диагностикой результатом применения очередной системной диагностики является полное восстановление до приемлемого уровня нарушенных возможностей по обеспечению выполнения требований по защите информации.

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

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

σ — частота возникновения источников угроз в процессе определения потребностей и требований заинтересованной стороны для системы;

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

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

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

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

$T_{зад}$ — задаваемый период прогноза.

Примечание — Примеры переопределения этих исходных данных (согласно способу 1 из В.2.3), конкретизированные в приложении к выходным результатам и действиям процесса, приведены в Г.4.

Оценку вероятности нарушения требований по защите информации в системе $R_{наруш}$ в течение периода прогноза $T_{зад}$ вычисляют по формуле

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

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

В настоящем подразделе определены расчетные выражения для случая, когда значения средних времен системной диагностики $T_{\text{диаг}}$ и восстановления нарушенных возможностей по обеспечению выполнения требований по защите информации $T_{\text{восст}}$ равны, т. е. для этого случая $P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}}) = P_{\text{возд (1)}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$. Расчет для более общего случая, когда значения $T_{\text{диаг}}$ и $T_{\text{восст}}$ различны, осуществляется с использованием 4-го способа повышения адекватности моделей (см. В.2.3).

Возможны два варианта:

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

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{\text{возд (1)}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ отсутствия нарушений требований по защите информации в моделируемой системе в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле

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

Примечание — Формулу (В.2) используют для оценки риска отсутствия нарушений требований по защите информации в моделируемой системе при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по математической модели «черного ящика» при отсутствии какого-либо контроля (см. В.2.1).

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

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

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

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

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

$P_{\text{кон}}$ — вероятность отсутствия нарушений по защите информации после последнего системного контроля, вычисляемая по формуле (В.2), т. е.

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

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

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

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 это середина или конец задаваемого периода прогноза $T_{\text{зад}}$.

Примечание — Для расчетов $P_{\text{возд (2)}}$ возможны иные вероятностные меры — например, когда N вычисляется как действительное число, а не как целая часть.

В итоге вероятность отсутствия нарушений требований по защите информации 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 требований по защите информации в системе $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по обеспечению выполнения требований по защите информации в системе. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны в течение заданного периода прогноза при реализации технологии периодического системного контроля.

Примечание — В частном случае, когда период между контролями больше периода прогноза $T_{зад} < T_{меж}$, модель В.2.2 превращается в модель В.2.1 для прогноза риска нарушения требований по защите информации в системе при отсутствии какого-либо контроля.

В.2.3 Расчет риска для систем сложной структуры, комбинация и повышение адекватности моделей

Описанные в В.2.1 и В.2.2 модели применимы для проведения оценок, когда система представляется в виде «черного ящика» и когда значения времен системной диагностики и восстановления нарушенной целостности совпадают. В развитие моделей В.2.1 и В.2.2 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 сохранение выполнения требований по защите информации в системе, указывается характер их логического соединения. Если два элемента соединяются последовательно, что означает логическое соединение «И» (см. рисунок В.1), то в контексте защиты информации это интерпретируется так: «система обеспечивает выполнение требований по защите информации в течение времени t, если «И» 1-й элемент, «И» 2-й элемент сохраняют свои возможности по обеспечению выполнения требований по защите информации 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 обеспечению выполнения требований по защите информации в течение времени t, если «ИЛИ» 1-й элемент, «ИЛИ» 2-й элемент сохраняют свои возможности по обеспечению выполнения требований по защите информации в течение этого времени».



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

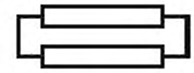


Рисунок В.2 — Система из параллельно соединенных элементов («ИЛИ»)

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

- для моделируемой системы из двух последовательно соединенных элементов

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

- для моделируемой системы из двух параллельно соединенных элементов

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

где $P_m(t)$ — вероятность нарушения требований по защите информации m-го элемента за заданное время t, $m = 1, 2$.

Примечание — Если для нарушения требований по защите информации нарушитель вынужден преодолевать несколько преград, это моделируется с использованием параллельно соединяемых элементов. Для

двух преград логическое соединение «ИЛИ» (см. рисунок В.3) интерпретируется так: система защиты из двух преград сохраняет свои возможности по обеспечению выполнения требований по защите информации в течение времени t, если 1-я преграда «ИЛИ» 2-я преграда сохраняют свои возможности по обеспечению выполнения требований по защите информации в течение этого времени, не позволяя нарушителю достичь своей цели вопреки преградам».

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.2.1 или В.2.2 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 требований по защите информации за время t для объединяемых подсистем. И так — до объединения на уровне системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (В.6) или (В.7) от исходных параметров моделей В.2.1 и В.2.2.

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.2.1 и В.2.2 и применения 2-го способа получается вероятность нарушения требований по защите информации 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 требований по защите информации 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 требований по защите информации каждого из элементов и системы в целом. С точки зрения системной инженерии это среднее время интерпретируют как виртуальную среднюю наработку на нарушение требований по защите информации в процессе определения потребностей и требований заинтересованной стороны при прогнозировании риска по моделям В.2.1 и В.2.2 для системы простой и сложной структуры. Обратная величина этого среднего времени — частота нарушений требований по защите информации в условиях определенных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения требований по защите информации для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей В.2.1 и В.2.2 или аналогичных 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.2.1 и В.2.2 в части учета времени на восстановление после нарушения требований по защите информации. В моделях В.2.1 и В.2.2 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 обеспечению выполнения требований по защите информации в течение времени $T_{восст}$, то для расчетов усредненное время контроля $T_{диаг}$ должно быть увеличено (если $T_{диаг} < T_{восст}$) или уменьшено (если $T_{диаг} > T_{восст}$). При этом усредненное время контроля вычисляют итеративно с заданной точностью:

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

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

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

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

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

где $R^{(r-1)}$ вычисляют по моделям В.2.1, В.2.2, но в качестве исходного уже выступает $T_{прим}^{(r-1)}$, 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 $T_{прим}^{(r)}$ сходится, и для дальнейших расчетов используют значение, отличающееся от точного предела $T_{прим}^{(\infty)}$ на величину, пренебрежимо малую по сравнению с задаваемой изначально точностью итерации ε:

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

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

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

$T_{восст}$ — среднее время восстановления нарушенной целостности моделируемой системы.

При этом для расчетов применяются одни и те же модели В.2.1 и В.2.2. В результате обеспечена возможность расчета показателей $P_{возд}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$, $T_{зад}$) и $R_{наруш}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$, $T_{зад}$) по формулам (В.1)—(В.7).

Примечание — Способ итеративного применения процессов рекомендован ГОСТ Р 57102.

Применение инженерных способов 1—4 обеспечивает более точный прогноз вероятности нарушения требований по защите информации для системы сложной структуры. Этой расчетной вероятности нарушения требований по защите информации в системе при оценке рисков сопоставляют возможный ущерб.

В.3 Прогнозирование рисков нарушения надежности реализации процесса без учета требований по защите информации

В.3.1 Общие положения

В.3.1.1 Модели В.3 ориентированы на контекст обеспечения надежности реализации процесса и использование математической формализации В.2 с учетом того, что надежность реализации процесса определения потребностей и требований заинтересованной стороны представляет собой свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях реализации.

В.3.1.2 В моделях для анализа надежности под системой понимают отдельное действие или множество действий процесса, выполняемых с использованием определенных защищаемых активов. Для каждого из анализируемых действий возможно либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения этого действия.

В.3.1.3 В терминах системы, отождествляемой с выполняемыми действиями, под целостностью моделируемой системы понимается такое ее состояние, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза. С точки зрения вероятностного прогнозирования риска нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны пространство элементарных событий на временной оси образуют следующие основные состояния:

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

Надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы в течение задаваемого периода прогноза обеспечена, если в течение этого периода для всех элементов моделируемой системы (т. е. для всех последовательно осуществляемых действий, логически объединяемых условием «И») обеспечена их целостность. Это означает, что в течение периода прогноза для всех последовательно осуществляемых недублируемых действий будет наблюдаться элементарное состояние «Целостность элемента моделируемой системы сохранена».

В.3.2 Математическая модель для прогнозирования риска при отсутствии какого-либо контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением формализации по модели В.2.1, отличие состоит в логическом переопределении исходных данных для моделирования. Это означает применение способа 1 из В.2.3. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности моделируемой системы в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетный риск нарушения надежности реализации процесса в течение заданного периода прогноза при отсутствии какого-либо контроля. Также применимы методы повышения адекватности В.2.3.

Модель применяют для случая, когда в системе отсутствует какой-либо контроль (диагностика) целостности реализуемых действий процесса. Модель представляет собой частный случай моделей В.2.2 и В.3.3, если период между моментами контроля целостности системы больше периода прогноза.

В.3.3 Математическая модель для прогнозирования риска при реализации технологии периодического системного контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением математической формализации по модели В.2.2, отличие состоит в логическом переопределении исходных данных для моделирования согласно способу 1 из В.2.3. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности рассматриваемой системы в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетный риск нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны (без учета требований по защите информации) в течение заданного периода прогноза при реализации технологии периодического системного контроля. Применимы методы повышения адекватности из В.2.3.

Для расчета риска нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны применительно к рассматриваемой системе исходные данные формально переопределяют применительно к выполняемым действиям процесса и защищаемым активам:

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

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

$T_{меж}$ — время между окончанием предыдущего и началом очередного контроля целостности системы;

$T_{диаг}$ — длительность системного контроля или диагностики целостности системы;

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

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

Примечание — Несмотря на фактическую повторяемость названий исходных данных, их значения при моделировании по модели В.3 будут отличны от значений при моделировании по модели В.2, поскольку различны их природа, исходные данные, интерпретация и области приложений. Соответственно разными ожидаются и расчетные риски по этим моделям.

В итоге вероятность отсутствия нарушений целостности моделируемой системы в течение периода прогноза $T_{зад}$ формально определяется теми же аналитическими выражениями (В.1)—(В.9), что и в моделях В.2.2, В.2.3, в зависимости от идентичных используемых исходных данных.

Сопоставление с возможным ущербом позволяет рассматривать формулу (В.1) как риск нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны системы $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$, в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления целостности. Эта расчетная вероятность интерпретируется как риск нарушения целостности системы в течение заданного периода прогноза. При этом требования по защите информации не учтены.

В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель В.3.3 превращается в модель В.3.2 для прогноза риска нарушения целостности моделируемой системы при отсутствии какого-либо контроля.

Примечания

1 Практическая адаптация и реализация моделей согласно положениям В.1—В.3 в приложении к системам дистанционного контроля промышленной безопасности в опасном производстве приведены в ГОСТ Р 58494.

2 Аналогичные модели для прогнозирования риска нарушения надежности реализации различных процессов более детально описаны в ГОСТ Р 59331—2021 (В.2 приложения В), ГОСТ Р 59333—2021 (В.2 приложения В), ГОСТ Р 59338—2021 (В.2 приложения В), ГОСТ Р 59347—2021 (В.2 приложения В).

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

Интегральную вероятность нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации $R_{1интегр.уч}(T_{зад})$ для различных прогнозных периодов определяют по формуле

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

Здесь $R_{1надежн}(T_{зад.над})$ — вероятность нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны в течение периода прогноза $T_{зад.над}$ без учета требований по защите информации, рассчитывается по моделям В.3 в зависимости от целей системного анализа;

$R_{1\text{наруш}}(T_{\text{зад.треб}})$ — вероятность нарушения требований по защите информации в системе для процесса определения потребностей и требований заинтересованной стороны в течение периода прогноза $T_{\text{зад.треб}}$, рассчитывается по формулам (В.1)—(В.9) в зависимости от целей системного анализа;

$T_{\text{зад.над}}$ — задаваемая длительность периода прогноза для анализа надежности реализации процесса определения потребностей и требований заинтересованной стороны;

$T_{\text{зад.треб}}$ — задаваемая длительность периода прогноза для анализа соблюдения требований по защите информации для процесса определения потребностей и требований заинтересованной стороны (на практике требования к срокам соблюдения требований по защите информации $T_{\text{зад.треб}}$ могут существенно превышать длительность непосредственно реализации процесса $T_{\text{зад.над}}$;

$T_{\text{зад}}$ — множество задаваемых периодов прогноза, характеризуемое двумя периодами прогноза: длительностью непосредственно реализации процесса определения потребностей и требований заинтересованной стороны $T_{\text{зад.над}}$ и длительностью соблюдения требований по защите информации $T_{\text{зад.треб}}$, т. е. $T_{\text{зад}} = (T_{\text{зад.над}}; T_{\text{зад.треб}})$.

Расчет $R_{1\text{надежн}}(T_{\text{зад.над}})$ и $R_{1\text{наруш}}(T_{\text{зад.треб}})$ вычисляют по формулам (В.1)—(В.9).

Расчет интегрального риска вычисляют по формуле (В.10).

Примечание — Использование «1» в нижних индексах показателей $R_{1\text{интегр.уч}}(T_{\text{зад}})$, $R_{1\text{надежн}}(T_{\text{зад.над}})$, $R_{1\text{наруш}}(T_{\text{зад.треб}})$ подчеркивает, что расчеты относятся к одной заинтересованной стороне. Если системные решения для различных заинтересованных сторон существенно разнятся, то, учитывая различие в исходных данных, возможно проведение расчетов для «j»-й заинтересованной стороны, $j = 1,\ldots, J$, $J > 1$. В этом случае вместо «1» используется индекс «j» — см. Г.5.

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса определения потребностей и требований заинтересованной стороны

Г.1 Общие положения

Г.1.1 Настоящие методические указания содержат типовые действия при расчетах основных количественных показателей рисков в процессе определения потребностей и требований заинтересованной стороны для системы:

- риска нарушения требований по защите информации;
- риска нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны для системы без учета требований по защите информации;
- интегрального риска нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации.

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

Г.1.2 Прогнозирование рисков осуществляют с использованием формализованного представления рассматриваемой системы в виде моделируемой системы. Под моделируемой системой понимается такая 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, множество активов и/или выходных результатов процесса, действия процесса или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях.

Г.1.3 Модели приложения В ориентированы на процесс определения потребностей и требований заинтересованной стороны для системы в случае, когда для различных заинтересованных сторон системные решения идентичны. В Г.5 приведены расчетные соотношения, позволяющие осуществлять прогнозирование интегрального риска применительно к случаю, когда системные решения для различных заинтересованных сторон существенно разнятся (например, это могут быть решения для обработки открытой и закрытой информации в системе).

Г.1.4 Применительно к конкретной системе для прогнозирования рисков нарушения требований по защите информации согласно 5.3, 6.1 определению подлежат:

- состав заинтересованных сторон, участвующих в формировании своих потребностей и требований к системе;
- состав выходных результатов и выполняемых действий процесса определения потребностей и требований заинтересованной стороны для системы и используемых при этом активов;
- перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для выходных результатов и выполняемых действий процесса определения потребностей и требований заинтересованной стороны для системы;
- технологии противодействия угрозам, используемые в процессе определения потребностей и требований заинтересованной стороны в заданной среде применения системы;
- иные объекты, используемые в прогнозировании рисков при необходимости оценки того, насколько организация способна обеспечить возможности по выполнению рассматриваемого процесса в заданной среде применения системы.

Примечание — В качестве конкретной системы может выступать система дистанционного контроля в опасном производстве (СДК). Для понимания основных идей по прогнозированию рисков см., например, ГОСТ Р 58494, где на примере СДК указаны объекты, выходные результаты, выполняемые действия, перечень потенциальных угроз применительно к объектам опасного производства.

Г.1.5 В зависимости от целей прогнозирования рисков модели, приведенные в В.2, В.3, логически могут быть представлены в виде «черного ящика» или в виде сложной структуры. Для отдельных элементов сложной системы или при ее огрубленном моделировании используют модель «черного ящика». Для получения более точных результатов прогнозирования рисков осуществляют декомпозицию сложной моделируемой системы до уровня составных системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых для описания целостности моделируемой системы логическими условиями «И» и «ИЛИ». При этом целостность моделируемой системы в течение задаваемого периода прогноза означает такое состояние этой системы, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза.

Примечания

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

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

Г.2 Цель прогнозирования рисков

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

Г.3 Элементарные состояния моделируемой системы

Для решения задач системного анализа в качестве моделируемой системы могут выступать: множество выходных результатов, множество действий процесса, множество заинтересованных сторон, объединенных целевым назначением в реальной системе.

Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи системного анализа. В общем случае моделируемую систему представляют либо в виде «черного ящика» (см. В.2.1 и В.2.2), либо в виде сложной системы, элементы которой объединяются соединяемых последовательно или параллельно (см. В.2.3). Пример декомпозиции сложной системы до составных элементов представлен на рисунках Г.1—Г.3. При этом для каждого элемента могут оказаться характерными свои разнородные угрозы и применяемые методы контроля, мониторинга и восстановления нарушаемой целостности.



Рисунок Г.1 — Пример моделируемой системы, представляющей собой множество выходных результатов, где системный элемент — это конкретный выходной результат (всего *I* выходных результатов)



Рисунок Г.2 — Пример моделируемой системы, представляющей собой множество действий процесса, где системный элемент — это конкретное действие (последнее *K*-е действие задублировано)



Рисунок Г.3 — Пример моделируемой системы, представляющей собой множество заинтересованных сторон, участвующих в формировании своих потребностей и требований к системе. Системный элемент — это конкретная заинтересованная сторона (всего *J* заинтересованных сторон)

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

Например, если системные решения для различных заинтересованных сторон идентичны, то в приложении к прогнозированию риска нарушения требований по защите информации для некоторой заинтересованной стороны пространство элементарных состояний на временной оси образуют два основных состояния:

- «Выполнение требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации, т. е. если выполняются все условия, интерпретируемые в совокупности как допустимая «норма»;

- «Выполнение требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы нарушено» — в противном случае.

Если системные решения для различных заинтересованных сторон по-прежнему идентичны, то в приложении к прогнозированию интегрального риска нарушения реализации процесса с учетом требований по защите информации для некоторой заинтересованной стороны пространство элементарных состояний на временной оси образуют два других основных состояния:

- «Надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены «И» надежность выполнения действий процесса, «И» выполнение требований по защите информации;

- «Надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы «И»/«ИЛИ» выполнение требований по защите информации в системе нарушены» — в противном случае.

Если же системные решения для различных заинтересованных сторон существенно разнятся, то для всего множества заинтересованных сторон в приложении к прогнозированию интегрального риска пространство элементарных состояний на временной оси будут определять следующие два состояния:

- «Для всех заинтересованных сторон надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза для каждой из заинтересованных сторон обеспечены «И» надежность выполнения действий процесса, «И» выполнение требований по защите информации;

- «Для полного множества заинтересованных сторон надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы «И»/«ИЛИ» выполнение требований по защите информации в системе нарушено» — в противном случае, т. е. если хотя бы для одной заинтересованной стороны имеет место нарушение «И»/«ИЛИ» надежности реализации процесса, «И»/«ИЛИ» выполнения требований по защите информации.

В общем случае с применением 1-го способа В.2.3 возможно расширение или переименование самих элементарных состояний, главное, чтобы они формировали полное множество аналогично множествам, введенным в настоящем подразделе. В Г.10.1, Г.10.2 приведены примеры прогнозирования рисков.

В качестве мер противодействия угрозам, способных при их применении снизить расчетные риски, могут выступать более частая (по сравнению со временем развития угроз) системная диагностика или контроль с восстановлением нормального функционирования моделируемой системы. Многократные прогнозы для реальных случаев нарушений нормы «до» и «после» наступления нарушений позволяют (при использовании задаваемых границ допустимого риска) осуществление аналитического обоснования упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижению затрат и/или возможных ущербов при задаваемых ограничениях. Обоснованное определение сбалансированных системных мер, предупреждающих возникновение ущербов при ограничениях на ресурсы и допустимые риски, а также оценка и обоснование эффективных кратко-, средне- и долгосрочных планов по обеспечению безопасности осуществляют путем решения самостоятельных оптимизационных задач, использующих расчетные значения прогнозируемых рисков — см. приложение Е.

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

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

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

Г.4 Показатели, исходные данные и расчетные соотношения

В общем случае для различных заинтересованных сторон системные решения могут существенно различаться (например, для обработки открытой и закрытой информации). Это должно быть учтено при решении некоторых задач системного анализа. В настоящем разделе приведены показатели, исходные данные и расчетные соотношения для одной j-й заинтересованной стороны ($j = 1,\ldots, J$) или, если системные решения для группы заинтересованных сторон идентичны, то для этой группы.

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

$R_{j\,\text{наруш}}(T_{\text{зад.треб}})$ — риск нарушения требований по защите информации в процессе определения потребностей и требований j-й заинтересованной стороны для системы в течение задаваемого периода прогноза $T_{\text{зад.треб}}$;

$R_{j\,\text{надежн}}(T_{\text{зад.над}})$ — риск нарушения надежности реализации процесса определения потребностей и требований j-й заинтересованной стороны для системы в течение задаваемого периода прогноза $T_{\text{зад.над}}$ без учета требований по защите информации;

$R_{j\ интегр.уч}(T_{зад})$ — интегральный риск нарушения реализации процесса определения потребностей и требований j-й заинтересованной стороны для системы с учетом требований по защите информации для различных задаваемых периодов прогноза $T_{зад.треб}$ (в части защиты информации) и $T_{зад.над}$ (в части надежности);

$T_{зад}$ — множество из двух задаваемых периодов прогноза ($T_{зад.над}$; $T_{зад.треб}$).

Применительно к моделируемой системе, отождествляемой с множеством выходных результатов процесса определения потребностей и требований j-й заинтересованной стороны для системы, для прогнозирования вероятностных показателей нарушения требований по защите информации $R_{j\ наруш}(T_{зад.треб})$ исходными данными по каждому составному элементу (т. е. для задействованных активов и получаемым выходным результатам) являются:

σ — частота возникновения источников угроз нарушения требований по защите информации применительно к системному элементу (например, выходному результату, зависящему от конкретных задействованных активов);

β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации применительно к системному элементу (выходному результату, зависящему от конкретных задействованных активов);

$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации применительно к системному элементу (выходному результату, зависящему от конкретных задействованных активов), определяется регламентом работы системы защиты информации);

$T_{диаг}$ — среднее время системной диагностики (контроля) состояния системного элемента (например, активов и самой системы защиты информации). В общем случае, это время, отличающееся от времени восстановления после выявления нарушений информационной безопасности. Это время определяется регламентом работы системы защиты информации и выполнением иных предусмотренных мер противодействия угрозам;

$T_{восст}$ — среднее время восстановления нормы эффективности защиты информации в системном элементе после выявления нарушений, определяется возможностями системы в части восстановления нормальных условий своего функционирования, включая выполнение требований по защите информации;

$T_{зад.треб}$ — задаваемая длительность периода прогноза для анализа соблюдения требований по защите информации.

Примечания

1 Для определения значений исходных данных σ и β сначала устанавливают условия допустимой «нормы» требований по защите информации, нарушение которых может приводить к недопустимому ущербу. После этого искусственно вводят условные границы для элементарного состояния системных элементов (в качестве элемента моделируемой системы здесь выступают задействованные активы и получаемый выходной результат), например:

- «приемлемое» состояние в пределах условий допустимой «нормы» требований по защите информации (частота выхода за пределы «приемлемого» состояния означает частоту возникновения источника угрозы, тем самым определяется значение σ);

- временное отклонение от «приемлемого» состояния, но в пределах условий допустимой «нормы» требований по защите информации (среднее время с момента выхода за пределы «приемлемого» состояния до нарушения условий допустимой «нормы» позволяет определить среднее время развития угроз, тем самым определяется значение β).

2 Как пример, для оборудования объектов опасного производства по ГОСТ Р 58494 границы «приемлемого» состояния определяют по границам рабочего диапазона значений отслеживаемых параметров оборудования (температуры, давления, напряжения и др.). Границы «нормы» определяются гарантийными обязательствами поставщиков оборудования. Между этими границами возможно временное отклонение от «приемлемого» состояния. В общем случае условные границы для элементарного состояния элементов могут быть не только количественными, но и качественными или только качественными (например, используют шаблон обязательных требований, к ним в зависимости от приложения добавляют или из них исключают некоторые условия, требующие неукоснительного выполнения).

Применительно к моделируемой системе, отождествляемой с выполняемыми действиями в процессе определения потребностей и требований j-й заинтересованной стороны (т. е. в данном случае в качестве элементов моделируемой системы выступают отдельные действия или совокупности действий, объединенных для анализа как один элемент), для прогнозирования вероятности нарушения надежности реализации процесса без учета требований по защите информации $R_{j\ надежн}(T_{зад.над})$ исходными данными по каждому составному элементу являются:

σ — частота возникновения источников угроз нарушения надежности системного элемента (т. е. реализации действия процесса);

β — среднее время развития угроз с момента возникновения источников угроз до наступления инцидента, связанного с нарушением надежности системного элемента (реализации действия процесса);

$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по обеспечению надежности системного элемента (реализации действия процесса) определяется регламентом работы системы контроля и управления надежностью;

$T_{диаг}$ — длительность системной диагностики надежности системного элемента (в общем случае отличающееся от времени восстановление после нарушений надежности), это время определяется регламентом работы системы контроля и управления надежностью и выполнением иных предусмотренных мер противодействия угрозам;

$T_{восст}$ — среднее время восстановления требуемой надежности системного элемента после наступления инцидента, связанного с нарушением надежности (реализации действия процесса), определяется возможностями системы контроля и управления надежностью в части восстановления нормальных условий своего функционирования;

$T_{зад.над}$ — задаваемая длительность периода прогноза для анализа надежности реализации процесса.

Если системные решения для различных заинтересованных сторон идентичны, то для математического моделирования используют расчетные соотношения (В.10), определенные формулами (В.1)—(В.9) для моделей В.2.3, В.2.4 и В.3.

Если системные решения для различных заинтересованных сторон существенно различаются, то исходные данные — те же, отличие лишь в их значениях и расчетных соотношениях, интегрирующих результаты расчетов $R_{j\ интегр.уч}(T_{зад})$ по всем $j = 1,..., J$. Расчетные соотношения для этого случая приведены в Г.5.

Г.5 Расчет интегрального риска для всех заинтересованных сторон (при различиях в системных решениях)

При различиях в системных решениях интегральный риск нарушения реализации процесса определения потребностей и требований всех заинтересованных сторон для системы с учетом требований по защите информации $R_{(1\ -\ J)\ интегр.уч}(T_{зад})$ для задаваемых периодов прогноза вычисляют по формуле

$$R_{(1-J)\,интегр.уч}(T_{зад}) = 1 - \prod_{j=1}^{J}[1 - R_{j\,интегр.уч}(T_{зад})] \qquad (Г.1)$$

Здесь $R_{j\ интегр.уч}(T_{зад})$ — риск нарушения надежности реализации процесса определения потребностей и требований j-й заинтересованной стороны в течение периодов прогноза $T_{зад}$ с учетом требований по защите информации, рассчитывается по расчетным соотношениям (В.10);

$T_{зад}$ — множество задаваемых периодов прогноза ($T_{зад.над}$; $T_{зад.треб}$), характеризуемое двумя периодами: длительностью периода прогноза для анализа непосредственно реализации процесса определения потребностей и требований заинтересованной стороны $T_{зад.над}$ и длительностью периода прогноза для анализа выполнения требований по защите информации $T_{зад.треб}$.

Примечание — При решении различных задач системного анализа, включая поддержку принятия решений, наряду с прогнозированием рисков с использованием выражений (В.1)—(В.11) возможно прогнозирование эффективности реализации процесса. Прогноз эффективности при этом направляют на вероятностную оценку того, насколько выполнение формализованных требований к системе способно обеспечить удовлетворение потребностей пользователей и других заинтересованных сторон в заданной среде применения системы.

Г.6 Порядок прогнозирования рисков

Г.6.1 Для прогнозирования рисков осуществляют следующие шаги.

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

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

Шаг 3. Формируют перечень возможных угроз. Принимают решение о представлении моделируемой системы в виде «черного ящика» или в виде сложной структуры, декомпозируемой до составных элементов с использованием логических условий «И», «ИЛИ». Формируют пространство элементарных состояний для каждого элемента и моделируемой системы в целом — действия осуществляют согласно Г.3.

Шаг 4. Выбирают расчетные показатели (риск нарушения требований по защите информации и/или интегральный риск нарушения реализации процесса с учетом требований по защите информации). Выбирают подходящие математические модели и методы повышения их адекватности из В.2, В.3, В.4. Устанавливают необходимость дифференциации заинтересованных лиц по группам (1,..., j,..., J) для прогнозирования рисков в случае, если

системные решения для различных заинтересованных сторон существенно разнятся. Формируют исходные данные для каждого элемента моделируемой системы. Осуществляют расчет выбранных показателей с использованием расчетных соотношений (В.1)—(В.11), а также согласно рекомендациям Г.4, Г.5.

Шаг 5. Результаты прогнозирования используют для оценки рисков и применяют для решения задач системного анализа согласно поставленным целям прогнозирования.

Г.6.2 Условия моделирования, исходные данные и полученные результаты прогнозирования рисков подлежат документированию.

Г.7 Обработка и использование результатов прогнозирования

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

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

Г.8 Примеры

Г.8.1 Нижеследующие примеры применительно к некоторой компании топливно-энергетического комплекса призваны продемонстрировать отдельные аналитические возможности методов и моделей настоящего стандарта. Пусть руководство компании, предпринимая меры по повышению уровня промышленной и информационной безопасности производства (см. [1]—[3], [9]—[12], [15]) и доверия бизнесу компании, приняло решение о проведении системного анализа, посвященного вопросам создания системы дистанционного контроля промышленной безопасности опасных производственных объектов. В общем случае применение СДК нацелено на оперативное выявление и оповещение ответственных лиц о предпосылках возникновения либо о возникновении опасных ситуаций на производственных объектах, удаленную информационно-аналитическую поддержку в интересах обеспечения нормальных условий функционирования производственных объектов и реализации на предприятиях риск-ориентированного подхода путем расчета и представления в режиме реального времени показателей состояния промышленной безопасности эксплуатируемого оборудования.

Именно СДК рассматривается в примерах в качестве моделируемой системы. Пример 1 посвящен прогнозированию риска нарушения требований по защите информации, пример 2 иллюстрирует прогнозирование риска нарушения надежности реализации процесса с учетом требований по защите информации, пример 3 демонстрирует учет требований различных заинтересованных сторон.

Г.8.2 Пример 1. Прогнозирование риска нарушения требований по защите информации проиллюстрировано для следующих выходных результатов процесса определения потребностей и требований заинтересованной стороны (см. 6.1.2):

- формализованных требований, отражающих потребности заинтересованных сторон в СДК;
- отчет о прослеживаемости сформулированных требований;
- характеристики и условия использования возможностей системы, критические показатели ее функционирования.

В компании выбор выходных результатов для системного анализа был обусловлен использованием следующих задействованных активов (защищаемых по-разному): финансовых и плановых документов, документации по обследованию объекта автоматизации, отчетов научно-исследовательских работ, баз данных (включая персональные данные должностных лиц), систем передачи данных, архивов компании — см. приложение А.

С учетом возможных ущербов в условиях существующей неопределенности цели прогнозирования рисков сформулированы руководством компании следующим образом:

цель 1 — количественно оценить риски нарушения требований по защите информации для каждого из выходных результатов и всей совокупности выходных результатов;

цель 2 — определить такой период, при котором сохраняются гарантии удержания риска в допустимых пределах для обеспечения нормы эффективности защиты информации;

цель 3 — определить критичные условия в развитии различных угроз.

Тем самым выполнены шаги 1, 2 настоящих методических указаний.

Выполняя шаг 3, выявлены критичные угрозы, влияющие на безопасность выходных результатов, основными из которых определены: угрозы, связанные с субъективными факторами, угрозы возникновения ущерба репутации и/или потери доверия из-за нарушения безопасности информации, угрозы безопасности функционирования программного обеспечения (ПО) оборудования и коммуникаций (см. приложение Б). Аналитиком моделируемой системы принято решение о формализованном представлении системы в виде сложной структуры — см. рисунок Г.4. Пространство элементарных состояний для каждого элемента и моделируемой системы из трех элементов сформировано согласно В.2 и Г.3 (элемент представляет собой конкретный выходной результат с задействованными для его получения активами). Определено элементарное состояние «Выполнение требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации для каждого из выходных результатов (с задействованными для их получения активами).



Рисунок Г.4 — Моделируемая система для примера 1

Выполняя шаг 4 методических указаний, на основании модели угроз безопасности информации, результатов обследования производственных объектов и технологий обеспечения информационной и промышленной безопасности сформированы приблизительные исходные данные для каждого элемента моделируемой системы, приведенные в таблице Г.1. Расчет риска нарушения требований по защите информации осуществлен с использованием расчетных соотношений (В.1)—(В.9) согласно рекомендациям Г.4, В.2.2 и В.2.3.

Таблица Г.1 — Исходные данные для прогнозирования риска нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны

Исходные данные	Значения и комментарии		
	для 1-го элемента	для 2-го элемента	для 3-го элемента
σ — частота возникновения источников угроз	Один раз в год (угрозы, связанные с субъективными факторами)	Один раз в год (угрозы возникновения ущерба репутации и/или потери доверия)	Один раз в месяц (угрозы безопасности ПО, оборудования и коммуникаций)
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	2 нед (развитие угроз может привести к неучету, несвоевременному или неадекватному учету потребностей)	1 мес, что соизмеримо со временем юридического разбирательства (развитие угроз может привести к возникновению ущерба репутации и/или потере доверия)	10 дней, что соизмеримо со временем разработки, модификации или адаптации ПО (развитие угроз может привести к нарушению качества и безопасности функционирования объекта)
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	1 ч (определяется регламентом контроля целостности ПО и активов)	1 ч (определяется регламентом контроля целостности ПО и активов)	1 ч (определяется регламентом контроля целостности ПО и активов)
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы защиты информации	30 с	30 с	30 с
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	5 мин (включая перезагрузку ПО и восстановление данных)	5 мин (включая перезагрузку ПО и восстановление данных)	5 мин (включая перезагрузку ПО и восстановление данных)
$T_{зад.треб}$ — задаваемая длительность периода прогноза	От полугода до двух лет (для определения периода, при котором сохраняются гарантии удержания риска в допустимых пределах для обеспечения нормы эффективности защиты информации)		

Выполняя шаг 5, проведена оценка рисков. Анализ результатов расчетов с учетом возможных ущербов показал, что в вероятностном выражении риск нарушения требований по защите информации в приложении ко всем выходным документам в течение года (т. е. для периода прогноза, равного 12 мес) функционирования СДК не превысит 0,035, составляя для 1-го выходного результата 0,0016, для 2-го выходного результата — 0,0007, для 3-го выходного результата — 0,0266 (структуру моделируемой системы см. на рисунке Г.4). Тем самым достигнута 1-я цель прогнозирования.

По всей совокупности выходных результатов компанией в качестве одной из норм эффективности защиты информации определен вероятностный уровень допустимого риска нарушения требований по защите информации в течение года, не превышающий 0,05. Анализ результатов расчетов показал, что максимальный период прогноза, при котором сохраняются гарантии удержания риска в допустимых пределах, составляет около 19 мес — см. зависимость на рисунке Г.5.



Рисунок Г.5 — Зависимость риска в приложении ко всем выходным результатам от длительности периода прогноза (от 6 до 24 мес)

С точки зрения обеспечения эффективности защиты информации этот результат прогнозирования интерпретируется так: для моделируемой системы гарантии удержания риска в допустимых пределах будут обеспечены в течение максимум 19 мес. Этот временной запас гарантирован с вероятностью не ниже 0,95, что в 19 раз превышает уровень допустимого риска (0,95/0,05 = 19). Тем самым достигнута 2-я цель прогнозирования.

Учитывая, что наиболее высокий риск ожидается для 3-го выходного результата, проведены дополнительные математические расчеты по определению критичных условий в развитии угроз безопасности функционирования программного обеспечения оборудования и коммуникаций (другие угрозы характеризуются на порядок меньшими рисками). Результаты расчетов показали: при изменении среднего времени развития угроз (β) от 5 до 20 сут риск нарушения требований по защите информации $R_{1\text{нарушт}}$ ($T_{\text{зад.треб}}$ = 1 год) убывает монотонно от 0,052 до 0,010, достигая условную границу 0,05 при значении β = 5,5 сут — см. зависимость на рисунке Г.6.



Рисунок Г.6 — Зависимость риска для 3-го выходного результата в течение года от среднего времени развития угроз (от 5 до 20 сут)

Это позволяет обосновать следующую норму эффективности защиты информации: при допустимом риске, полагаемом равным 0,05, защита информации должна быть такой, чтобы с момента выявления признаков возникновения реальных угроз безопасности функционирования программного обеспечения оборудования и коммуникаций предпринимаемые меры обеспечения защиты позволяли отсрочивать возникновение ущерба вследствие нарушения требований по защите информации на 20 и более дней. Этот запас времени — одна из важных требуемых норм эффективности защиты информации. Тем самым достигнута последняя 3-я цель прогнозирования в рамках примера 1.

Г.8.3 Пример 2. В продолжение примера 1 прогнозирование интегрального риска нарушения реализации процесса определения потребностей и требований некоторой заинтересованной стороны с учетом требований по защите информации проиллюстрировано для следующих действий процесса (см. 6.1.3):

- определения потребностей заинтересованных сторон СДК;
- разработки концепции функционирования СДК;
- поддержки основных информационных активов, создаваемых в рамках процесса (должны быть установлены границы этого действия в рамках процесса определения потребностей и требований заинтересованной стороны, поскольку полная поддержка основных активов в их жизненном цикле относится к процессу функционирования).

В отличие от примера 1 цели прогнозирования интегрального риска с учетом возможных ущербов сформулированы иначе:

цель 1 — установить соотношение риска нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны (без учета требований по защите информации) и риска нарушения требований по защите информации;

цель 2 — определить такой период, при котором сохраняются гарантии удержания риска в допустимых пределах нарушения надежности реализации процесса (без учета требований по защите информации);

цель 3 — определить для реальной длительности процесса, насколько повысится риск нарушения надежности его реализации (без учета требований по защите информации) по сравнению с риском нарушения надежности его реализации с учетом требований по защите информации.

Вышеперечисленное отвечает выполнению первых двух шагов настоящих методических указаний.

В рамках шага 3 компанией определено, что для надежности выполнения имеют место те же основные угрозы, что и в примере 1. Аналитиком моделируемой системы принято решение о формализованном ее представлении в виде сложной структуры — см. рисунок Г.7.

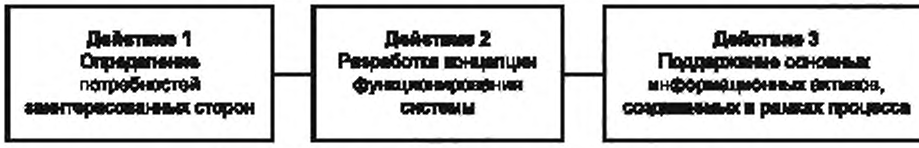


Рисунок Г.7 — Моделируемая система для примера 2

Пространство элементарных состояний для каждого элемента и моделируемой системы из трех элементов сформировано согласно В.2 и Г.3 (элемент представляет собой конкретное действие с использованием свойственных для него активов). Определено элементарное состояние: «Надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы обеспечена» (без учета требований по защите информации), если в течение всего периода прогноза обеспечена надежность реализации каждого из действий процесса. «Надежность реализации процесса определения потребностей и требований заинтересованной стороны для системы «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены «И» надежность выполнения действий процесса, «И» выполнение требований по защите информации для выходных результатов.

В рамках примера учтено, что во многих случаях применяемый процесс определения потребностей и требований заинтересованной стороны для конкретных систем занимает несколько суток или недель, а сами выработанные в результате реализации процесса требования сохраняются длительное время.

Примечание — Для систем коллективного пользования процесс определения потребностей и требований заинтересованной стороны может занимать несколько минут. Например, этот процесс может включать в себя регистрацию пользователей и установление фильтров для пользовательских запросов, а поддерживающее хранение результатов запросов отнесено к процессу функционирования.

Выполняя шаг 4 методических указаний, на основании модели угроз безопасности информации, результатов обследования производственных объектов и технологий обеспечения информационной и промышленной безопасности сформированы ориентировочные исходные данные для каждого элемента моделируемой системы, приведенные в таблице Г.2.

Расчет риска нарушения требований по защите информации с учетом специфики процесса осуществлен с использованием расчетных соотношений (В.1), (В.2), (В.6)—(В.9) согласно рекомендациям Г.4 с ориентацией на модели и методы В.2.2, В.2.3. Учтена специфика процесса: она заключается в относительной кратковременности и отсутствии периодического системного контроля, поскольку контроль проводится участниками процесса по ходу его выполнения. Это означает применимость модели В.3.2.

Выполняя шаг 5 методических указаний, проведена оценка рисков. Анализ результатов расчетов с учетом возможных ущербов показал, что в вероятностном выражении риск нарушения надежности реализации процесса в

течение 15 сут в приложении ко всем выполняемым действиям составит около 0,027 — см. рисунок Г.8, по каждому из действий — 0,0083. Вместе с тем риск нарушения требований по защите информации в течение тех же 15 сут составит около 0,0012, что рассчитано по исходным данным примера 1 для $T_{зад.треб}$ = 15 сут — см. рисунок Г.9.

Таблица Г.2 — Исходные данные для прогнозирования риска нарушения надежности реализации процесса (без учета требований по защите информации)

Исходные данные	Значения и комментарии		
	для 1-го элемента	для 2-го элемента	для 3-го элемента
σ — частота возникновения источников угроз нарушения надежности реализации процесса	Один раз в год, что соизмеримо с наработкой на ошибку специалистов высокой квалификации (угрозы, связанные с субъективными факторами, или угрозы возникновения ущерба репутации и/или потери доверия)	Один раз в год, что соизмеримо с наработкой на ошибку специалистов высокой квалификации (угрозы, связанные с субъективными факторами, или угрозы возникновения ущерба репутации и/или потери доверия)	Один раз в год, что соизмеримо с наработкой на ошибку специалистов высокой квалификации (угрозы безопасности функционирования программного обеспечения оборудования и коммуникаций)
β — среднее время развития угроз с момента возникновения источников угроз до наступления инцидента, связанного с нарушением надежности реализации процесса	1 мес, что соизмеримо со временем юридического разбирательства	1 мес, что соизмеримо со временем юридического разбирательства	1 мес, что соизмеримо со временем юридического разбирательства
$T_{зад.над}$ — задаваемая длительность периода прогноза	От 8 до 30 дней		



Рисунок Г.8 — Зависимость риска нарушения надежности реализации процесса (без учета требований по защите информации) от длительности периода прогноза



Рисунок Г.9 — Зависимость риска нарушения требований по защите информации от длительности периода прогноза

В итоге системного анализа установлено, что риск нарушения надежности реализации процесса определения потребностей и требований заинтересованной стороны (без учета требований по защите информации) в 22,5 раза превышает риск нарушения требований по защите информации. Первая цель прогнозирования в примере 2 достигнута.

Дополнительный анализ расчетной зависимости на рисунке Г.8 показал, что максимальный период прогноза, при котором сохраняются гарантии удержания риска в допустимых пределах 0,05, составляет около 22 сут. С точки зрения системной инженерии этот результат прогнозирования интерпретируется так: для моделируемой системы гарантии удержания риска в допустимых пределах будут обеспечены в течение максимум 22 сут. Этот временной запас гарантирован с вероятностью не ниже 0,95. Тем самым достигнута 2-я цель прогнозирования.

Для достижения 3-й цели осуществляются дополнительные расчеты по формуле (В.10) для задаваемого периода прогноза $T_{зад.над} = T_{зад.треб} = 15$ сут. Интегральный риск нарушения реализации процесса определения потребностей и требований заинтересованной стороны с учетом требований по защите информации составит = 0,0282 (подставляя в формулу (В.10), получается $1 – (1 – 0,027) \cdot (1 – 0,0012) = 0,0282$. Это означает, что интегральный риск нарушения реализации процесса с учетом требований по защите информации получит приращение на 4,3 % по сравнению с риском нарушения надежности реализации процесса без учета требований по защите информации (0,027). Тем самым достигнута последняя 3-я цель прогнозирования рисков в рамках примера 2.

Г.8.4 Пример 3 демонстрирует учет требований различных заинтересованных сторон при проведении оценки риска. Рассматриваются две заинтересованные стороны (см. рисунок Г.10):

- 1-я заинтересованная сторона, включающая руководство компании и должностных лиц, отвечающих за безопасность в компании;
- 2-я заинтересованная сторона, куда относятся государственные органы, осуществляющие надзор и контроль за состоянием безопасности.

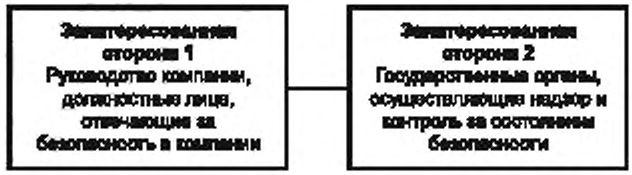


Рисунок Г.10 — Моделируемая система для примера 3

Для моделируемой системы «Надежность реализации процесса определения потребностей и требований всех заинтересованных сторон для системы «И» выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены «И» надежность выполнения действий процесса, «И» выполнение требований по защите информации для каждой из заинтересованных сторон.

Системные решения для 2-й заинтересованной стороны могут отличаться от системных решений для компании, поскольку государственные органы, осуществляющие надзор и контроль за состоянием безопасности, интересуют лишь состояние защищенности от угроз безопасности функционирования программного обеспечения оборудования и коммуникаций. Вместе с тем, для демонстрации работоспособности методики полагая, что оценки рисков для системных решений относительно обеих заинтересованных сторон приблизительно одинаковы и соответствуют результатам примера 2, т. е. $R_{1интегр. с учетом}(T_{зад}) = R_{2интегр. с учетом}(T_{зад}) = 0,00282$. Интегральный риск нарушения реализации процесса определения потребностей и требований всех заинтересованных сторон для системы с учетом требований по защите информации может быть оценен по формуле (Г.1). В итоге этот оцениваемый интегральный риск составит около 0,0056. Это получено в результате расчетов: $1 – (1 – 0,00282) \times (1 – 0,00282) = 0,0056$. С точки зрения системной инженерии результат прогнозирования интерпретируется так: для моделируемой системы надежная реализация процесса определения потребностей и требований всех заинтересованных сторон с выполнением требований по защите информации в системе в 177 раз более вероятна по сравнению с возникновением реальных нарушений (0,9944 против 0,0056).

Примечание — Другие примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Г.9 Материально-техническое обеспечение

В состав материально-технического обеспечения для прогнозирования рисков входят (в части, свойственной процессу определения потребностей и требований заинтересованной стороны для системы):

- результаты обследования, концепция создания, технический облик и/или ТЗ на разработку для создаваемой системы, конструкторская и эксплуатационная документация для рассматриваемой системы (используются при формировании необходимых исходных данных для моделирования);
- модель угроз безопасности информации (используется для формирования необходимых исходных данных 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 (используются при формировании необходимых исходных данных для моделирования);

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

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

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

Г.10 Отчетность

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

Приложение Д
(справочное)

Типовые допустимые значения показателей рисков для процесса определения потребностей и требований заинтересованной стороны

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

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

Требования системной инженерии при допустимых рисках, свойственных конкретной системе или ее аналогу и 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 выполнения процесса определения потребностей и требований всех заинтересованных сторон для системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

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

Таблица Д.1 — Пример задания допустимых значений рисков

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

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса определения потребностей и требований заинтересованной стороны

Е.1 Методика прогнозирования риска нарушения требований по защите информации в процессе определения потребностей и требований заинтересованной стороны для системы (охватывающая случаи, когда системные решения для различных заинтересованных сторон идентичны и существенно разнятся).

Е.2 Методика прогнозирования интегрального риска нарушения реализации процесса определения потребностей и требований заинтересованной стороны для системы с учетом требований по защите информации.

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

Е.4 Методики выявления явных и скрытых недостатков процесса определения потребностей и требований заинтересованной стороны для системы с использованием прогнозирования рисков.

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

Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения потребностей и требований заинтересованной стороны для системы.

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[19] 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), утвержденные приказом Председателя Гостехкомиссии России от 30 августа 2002 г. № 282

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

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

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

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

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

Ключевые слова: актив, безопасность, защита информации, модель, процесс определения потребностей и требований заинтересованной стороны, риск, система, системная инженерия, управление

Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 11.05.2021. Подписано в печать 24.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru