ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59335— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ЗНАНИЯМИ О СИСТЕМЕ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 апреля 2021 г. № 310-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 (www.gost.ru)

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе управления знаниями о системе 7
5 Общие требования системной инженерии по защите информации в процессе управления знаниями о системе 9
6 Специальные требования к количественным показателям 10
7 Требования к системному анализу 12
Приложение А (справочное) Пример перечня защищаемых активов 14
Приложение Б (справочное) Пример перечня угроз 15
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 16
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса управления знаниями о системе 25
Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса управления знаниями о системе 36
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса управления знаниями о системе 37
Библиография 38

Введение

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

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

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

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

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

Стандарт устанавливает основные требования системной инженерии по защите информации в процессе управления знаниями о системе и специальные требования к используемым количественным показателям.

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ЗНАНИЯМИ О СИСТЕМЕ

System engineering. Protection of information in knowledge management process about system

Дата введения — 2021—11—30

1 Область применения

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

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

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

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

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 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 19.101 Единая система программной документации. Виды программ и программных документов

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

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

Издание официальное

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

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

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

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 50779.41 (ИСО 7879—93) Статистические методы. Контрольные карты для арифметического среднего с предупреждающими границами

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

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

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

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

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

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

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

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

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

ГОСТ Р 57127 Менеджмент знаний. Руководство по наилучшей практике

ГОСТ Р 57133 Менеджмент организационной культуры и знания. Руководство по наилучшей практике

ГОСТ Р 57193—2016 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 58086 Интеллектуальная собственность. Распределение интеллектуальных прав между заказчиком, исполнителем и автором на охраняемые результаты интеллектуальной деятельности, создаваемые и/или используемые при выполнении научно-исследовательских, опытно-конструкторских, технологических и производственных работ

ГОСТ Р 58223 Интеллектуальная собственность. Антимонопольное регулирование и защита от недобросовестной конкуренции

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия).

Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 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 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508, 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, статья 2.3]

3.1.2

база знаний: объем знаний, доступный для организации.

Примечание — База знаний содержит квалификации, компетентность, коллективные и индивидуальные знания, поддерживаемые собранной информацией и данными. Организация может формировать специальные базы данных для сопоставления информации по ключевым направлениям (темам) или процессам.

[ГОСТ Р 53894—2016, статья 2.7]

3.1.3

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

[ГОСТ Р 51898—2002, пункт 3.7]

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

знания: Объем восприятий и навыков, которые придуманы людьми. Объем знаний увеличивается пропорционально поступающей информации.

Примечания

1 Существует множество контекстных определений знания:
- «сопряженные знания»;
- «ноу-хау»;
- «рабочие знания»;
- «неформализованные (неявные) знания».

2 Набор данных и информации (с точки зрения некоторой определенной информационной технологии). Включает также различные комбинации новой технологии, производственного опыта, эмоций, верований, значений величин, идей, интуиции, любопытства, мотивации, стилей обучения, отношения, способности доверять, способности решать сложные проблемы, открытости, умения работать в компьютерной сети, коммуникабельности, отношения к риску, наличия духа предпринимательства. Использование знаний приводит к накоплению ценных активов, улучшает способность действовать и принимать эффективные решения. В отличие от формализованного знания существует знание неформализованное. Оно также может быть индивидуальным и коллективным.

[ГОСТ Р 53894—2016, статья 2.20]

3.1.6

инновация: Применение новых или иных способов внедрения процессов, процедур или продукции, что достигается путем обеспечения пространства и возможности для новых идей.

Примечание — Организации часто используют менеджмент знаний для создания среды, которая способна стимулировать инновации путем предоставления качественного доступа к предыдущему опыту, стимулам и поддерживающим процессам для совместной работы и создания новых знаний.

[ГОСТ Р 53894—2016, статья 2.23]

3.1.7 **интегральный риск нарушения реализации процесса управления знаниями о системе 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.

3.1.8

менеджмент знаний: Дисциплинарный подход к достижению поставленных перед организацией целей путем оптимального использования знаний.

[ГОСТ Р 53894—2016, статья 2.36]

3.1.9

метаданные: Структурированная информация, которая описывает и (или) обеспечивает выявление, управление, контроль, понимание или сохранение информации в течение определенного времени.

[ГОСТ Р 53894—2016, статья 2.38]

3.1.10 **надежность реализации процесса управления знаниями о системе:** Свойство процесса управления знаниями о системе сохранять во времени в установленных пределах значения показателей, характеризующих способность приобретения и/или создания, распространения, своевременного применения и сохранения полезных знаний о системе в заданных условиях реализации процесса.

3.1.11 **полезные знания о системе:** Знания о системе, приобретение и/или создание и своевременное применение которых способно в заданных условиях принести пользу системе, другим системам, связанным с этой системой, и/или обеспечить удовлетворенность заинтересованных сторон.

3.1.12

ресурсы знаний, активы знаний: Формы интеллектуального капитала, которые объединяются для создания ценностей организации. Они включают в себя квалификации, основные процессы, человеческий потенциал, социальный капитал, связанные с работами знания, навыки и опыт, добросовестную практику, подбор сотрудников и поддержание успеха. Являются основой для формирования нематериальных активов.

[ГОСТ Р 53894—2016, статья 2.65]

3.1.13

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.14 **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.

3.1.15

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]

3.1.16 **скрытые угрозы системе:** Неявные угрозы, выявление которых осуществляют лишь по признакам, косвенно связанным с возможными реальными угрозами, а распознавание — путем оценки развития предпосылок к нарушению нормальных условий существования и/или функционирования системы.

3.1.17 **таксономия:** Учение о принципах и практике классификации и систематизации сложноорганизованных иерархически соотносящихся сущностей.

3.1.18

требование по защите информации: Установленное правило или норма, которые должны быть выполнены при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

[ГОСТ Р 50922—2006, статья 2.9.2]

3.1.19

угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

[ГОСТ Р 50922—2006, статья 2.6.1]

3.1.20 **управление знаниями:** Целенаправленное создание, приобретение, сохранение, распространение и применение знаний в заданных условиях в определенной области приложения.

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

3.1.22

центр знаний: Виртуальная территория или место работы сотрудников организации, где хранятся знания, к которым может быть обеспечен доступ посторонних лиц.

Примечание — Центрами знаний могут быть библиотеки, кафе, дискуссионные площадки или области неформальных собраний, которые стимулируют получение знаний и их распространение.

[ГОСТ Р 53894—2016, статья 2.90]

3.1.23

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.1.24 **явные угрозы системе:** Угрозы нормальным условиям существования и/или функционирования системы, однозначное выявление и распознавание которых возможно по заранее определенным и реально проявляемым свойственным признакам.

3.2 В настоящем стандарте использованы следующие сокращения:

ИТ — информационные технологии;

ТЗ — техническое задание;

ЦЗн — центр знаний.

4 Основные положения системной инженерии по защите информации в процессе управления знаниями о системе

4.1 Общие положения

Организации используют процесс управления знаниями о системе для повышения качества и/или безопасности создаваемой или применяемой системы, других систем, связанных с этой системой, и/или эффективности их применения. В процессе управления знаниями о системе осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

Для прогнозирования рисков нарушения надежности реализации процесса и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах используют системный анализ с учетом требований по защите информации.

Определение выходных результатов процесса управления знаниями о системе и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 7.32, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602,

ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Оценку интегрального риска нарушения реализации процесса управления знаниями о системе осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51897, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355 с учетом специфики создаваемой (модернизируемой) и/или применяемой или выводимой из эксплуатации системы — см., например [21] — [27].

4.2 Стадии и этапы жизненного цикла систем

Процесс управления знаниями о системе может быть использован на любой стадии жизненного цикла системы.

Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации систем устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования систем. Перечень этапов и конкретных работ в жизненном цикле систем формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839. Процесс управления знаниями о системе может входить в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости включать в себя другие процессы.

4.3 Цели процесса и назначение мер по защите информации

4.3.1 Определение целей процесса управления знаниями о системе осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508 в соответствии со спецификой, создаваемой (модернизируемой) и/или применяемой системы, планируемого проекта, организации, выполняющей проект, а также реализуемой стадии жизненного цикла системы. В общем случае главной целью процесса управления знаниями о системе является повышение качества и/или безопасности и/или эффективности системы или связанных с ней систем за счет приобретения, создания, распространения, своевременного применения и сохранения полезных знаний в их жизненном цикле.

Частными целями процесса управления знаниями о системе являются:

- при создании или приобретении знаний: получение новых знаний о системе, например в результате научно-исследовательских или опытно-конструкторских работ, или в рамках уже сложившихся и совершенствуемых технологических процессов внутри или вне рассматриваемой системы;
- при сохранении знаний: применение соответствующих мер защиты информации, используемой для формирования знаний, защиты самих знаний, баз знаний и носителей знаний от разнородных угроз;
- при распространении знаний: доведение знаний до потребителей для последующего целевого использования в системе;
- при применении знаний: повышение качества и/или безопасности и/или эффективности системы, связанных с ней систем и обеспечение удовлетворенности заинтересованных сторон.

Примечание — Условия сохранения знаний специалистов, являющихся непосредственными носителями знаний, их физической и социальной защиты определяются в соответствии с законодательством Российской Федерации.

4.3.2 Меры защиты информации в процессе управления знаниями о системе предназначены для обеспечения предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, формирующей знания и базы знаний, для защиты носителей знаний от разнородных угроз, способных привести к утрате знаний или несанкционированной передаче знаний третьей стороне. Определение мер по защите информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 56939, ГОСТ Р 58412, [19] — [24] с учетом специфики создаваемой или применяемой системы, планируемого проекта, организации, выполняющей проект, а также реализуемой стадии жизненного цикла системы.

4.4 Основные принципы

При проведении системного анализа процесса управления знаниями о системе 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 выполняемых действий.

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе управления знаниями о системе сосредотачивают:

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

5 Общие требования системной инженерии по защите информации в процессе управления знаниями о системе

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 каковой может выступать система защиты информации), в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например [1] — [27]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

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

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

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

Требования системной инженерии по защите информации в процессе управления знаниями о системе 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, обоснованию эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах.

5.3 Состав выходных результатов и выполняемых действий в процессе управления знаниями о системе определяют по ГОСТ 2.114, ГОСТ 7.32, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57127, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики создаваемой (модернизируемой) и/или применяемой системы.

Примечание — В процессе управления знаниями о системе необходимо учитывать решение таких вопросов, как:

- гарантированное подтверждение достаточности автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации и т.п.);

- учет возможности повышения уровня конфиденциальности данных в процессе их обработки в системах искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации и т.п.);
- регламентация вопросов обеспечения конфиденциальности тестовых выборок исходных данных, используемых испытательными лабораториями при оценке соответствия прикладных систем искусственного интеллекта, с сохранением прозрачности и подотчетности этого процесса.

5.4 Меры и действия по защите информации должны охватывать информационные активы и активы знаний, информация которых или о которых подлежит защите для получения выходных результатов и выполнения действий процесса управления знаниями о системе.

Примечание — В состав активов могут быть включены активы, используемые для достижения целей процесса управления знаниями о системе для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика, например привлекаемые средства контроля качества разрабатываемого программного обеспечения.

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ 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 57127, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508, [19] — [24].

Примеры перечней учитываемых активов и угроз в процессе управления знаниями о системе приведены в приложениях А и Б.

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

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, 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, [19] — [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 управления знаниями о системе определен в 6.3.

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

6 Специальные требования к количественным показателям

6.1 Общие положения

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

6.1.2 В общем случае основными выходными результатами процесса управления знаниями о системе являются:

- стратегия управления знаниями организации (техническое задание, планы, программы и методики, инструкции, руководства пользователя);
- таксономия для применения активов знаний;
- организационные знания и активы знаний;
- конкурентные преимущества организации;
- методы и технологии повышения эффективности;
- «ноу-хау» и инновации в отношении процессов жизненного цикла конкретных систем, инфраструктуры, архитектуры, новой продукции и программного обеспечения;
- результаты системного анализа в части обеспечения и повышения качества и/или безопасности, и/или эффективности применения конкретных систем и удовлетворенности заинтересованных сторон.

6.1.3 Для получения выходных результатов процесса управления знаниями о системе в общем случае выполняют следующие основные действия:

- определение потребностей в знаниях;
- определение стратегии управления знаниями (включая составление планов по получению и поддержанию активов знаний, определение механизмов и процедур для генерации новых знаний, защиты, контроля и доступа к информации и знаниям, хранения и поиска знаний, в том числе распространенных вне организации, среди заинтересованных сторон, приобретающих сторон и деловых партнеров);
- определение знаний, которые подлежат управлению;
- определение проектов, для которых может быть извлечена польза от применения знаний;
- создание или приобретение активов знаний;
- сохранение знаний, включая защиту активов знаний и иных активов, связанных со знаниями;
- распространение активов знаний по организации;
- сопровождение активов знаний;
- контроль и документирование использования активов знаний;
- переоценку технологической и рыночной стоимости активов знаний;
- оценку эффективности процесса управления знаниями;
- оценку эффективности функционирования организации с использованием процесса управления знаниями.

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 управления знаниями о системе с учетом требований по защите информации.

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

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе управления знаниями о системе используют следующие количественные показатели:

- риск нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации;

- риск нарушения требований по защите информации в процессе управления знаниями о системе;
- интегральный риск нарушения реализации процесса управления знаниями о системе с учетом требований по защите информации.

6.3.2 Риск нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации характеризуется соответствующей вероятностью в зависимости от нарушения надежности реализации процесса приобретения знаний, создания полезных знаний о системе и распространения приобретенных или созданных полезных знаний о системе (все без учета требований по защите информации) в сопоставлении с возможным ущербом.

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

6.3.4 Интегральный риск нарушения реализации процесса управления знаниями о системе характеризуется соответствующими вероятностями нарушения надежности приобретения и/или создания, распространения, нарушения своевременного применения и сохранения полезных знаний о системе без учета требований по защите информации и вероятностью нарушения требований по защите информации (см. В.2, В.3, В.4) в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

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

- 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 управления знаниями о системе, но и о событиях, связанных 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, характеризующих нарушения и предпосылки к нарушениям требований по защите информации и последовавших из-за этих ошибок) в самой системе или в системах-аналогах;
- данные из модели угроз безопасности информации и метаданные, позволяющие сформировать перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для каждого из защищаемых активов.

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к системному анализу

Требования к системному анализу процесса управления знаниями о системе включают:

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

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 3534-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 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 создаваемой (модернизируемой) и/или применяемой системы, планируемого или реализуемого проекта и организации, выполняющей проект, а также реализуемой стадии жизненного цикла системы.

Примечание — Примеры решения задач системного анализа применительно к процессу управления знаниями о системе приведены в приложении Г, а применительно к другим процессам — в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе управления знаниями о системе 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];
- ТЗ — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р 57839, с учетом специфики создаваемой (модернизируемой) и/или применяемой системы;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- конструкторскую и технологическую документацию — по ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201;
- эксплуатационную документацию (для модернизируемой или применяемой системы) — по ГОСТ 34.201, ГОСТ Р 2.601;
- документацию на автоматизированные системы — по ГОСТ 34.201;
- программную документацию — по ГОСТ 19.101;
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101 с учетом специфики создаваемой (модернизируемой) системы;
- программное обеспечение создаваемой и применяемой системы и средств его разработки и сопровождения;
- базу данных и базу знаний, систему хранения архивов;
- систему передачи данных и облачные данные организации;
- интеллектуальную собственность — по ГОСТ Р 58086, ГОСТ Р 58223;
- выходные результаты иных процессов в жизненном цикле системы с учетом ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

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

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275;
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124, ГОСТ Р 56939, ГОСТ Р 58412;
- угрозы безопасности информации при подготовке и обработке документов — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (разработчика, производителя) к конкретному заказчику, информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением знаний с использованием облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги;
- угрозы, связанные с нарушением интеллектуальной собственности, а также с несанкционированным распространением знаний о системе за пределы системы;
- угрозы, связанные с неопределенностью ответственности за обеспечение защиты информации в процессе управления знаниями о системе;
- угрозы распространения ложной информации о знаниях, используемых в организации;
- прочие соответствующие угрозы безопасности информации, связанные с человеческим фактором, 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 управления знаниями могут применяться любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. В настоящем приложении приведены модели и методы прогнозирования рисков, обеспечивающие вероятностную оценку следующих показателей:

- рисков нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации (см. В.2);
- риска нарушения требований по защите информации в процессе управления знаниями о системе (см. В.3);
- интегрального риска нарушения реализации процесса управления знаниями о системе с учетом требований по защите информации (см. В.4).

В.1.2 Риск нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации определяют соответствующей вероятностью в зависимости от нарушения надежности реализации процесса приобретения знаний, создания полезных знаний о системе и распространения приобретенных или созданных полезных знаний о системе (все без учета требований по защите информации).

Риск нарушения требований по защите информации в процессе управления знаниями о системе определяют соответствующей вероятностью нарушения требований по защите информации.

Вероятностные оценки обеспечивают уровень адекватности, достаточный для решения задач системного анализа, при условии многократной повторяемости анализируемых событий или в предположении такой повторяемости.

В.1.3 Интегральный риск нарушения реализации процесса управления знаниями о системе с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации и риска нарушения требований по защите информации в этом процессе.

В.1.4 При оценке рисков расчетным вероятностным показателям сопоставляют возможный ущерб, оцениваемый тяжестью последствий для системы и ее заинтересованных сторон в случае реализации угроз.

В.1.5 Для моделируемой системы нарушение реализации процесса управления знаниями о системе с учетом требований по защите информации характеризуется переходом моделируемой системы в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: из-за нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации либо из-за нарушения требований по защите информации, либо из-за комбинации перечисленных причин.

В.1.6 В общем случае, исходя из целей системного анализа, риски оценивают на разных исходных данных. При использовании одних и тех же моделей для расчетов это может приводить к различным оценкам и интерпретациям рисков. Различия связаны с неодинаковой тяжестью возможного ущерба для заинтересованных сторон, недоступностью или неполнотой статистических данных, используемых каждой из этих сторон в качестве исходных данных при системном анализе.

В.1.7 Выполнение или невыполнение действий и требований при моделировании отслеживается с использованием индикаторной функции $Ind(\alpha)$, которая позволяет учесть критичность последствий, связанных с невыполнением заданных условий согласно собираемой статистике

$$Ind(\alpha) = \begin{cases} 1, & \text{если условие } \alpha \text{ выполнено,} \\ 0, & \text{если условие } \alpha \text{ не выполнено.} \end{cases} \quad (В.1)$$

Условие α, используемое в индикаторной функции, формируют путем анализа выполнения конкретных условий.

В.1.8 При формировании исходных данных для моделирования и проведении разностороннего системного анализа используют статистические методы по ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р 50779.41, методы оценки рисков из настоящего приложения и/или по ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59349, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

В.1.9 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы или для системы, выбранной в качестве аналога. Для исследования запроектных сценариев, связанных с управлением знаниями, при моделировании могут быть использованы гипотетичные исходные данные.

В.2 Методы оценки рисков нарушения надежности реализации процесса без учета требований по защите информации

В.2.1 Общие положения

В настоящем подразделе приведены методы оценки частных и обобщенного рисков нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации.

Частные риски характеризуются сопоставляемыми возможными ущербами и вероятностями соответствующих событий:

- вероятностью нарушения надежности реализации процесса приобретения знаний без учета требований по защите информации;
- вероятностью нарушения надежности создания полезных знаний о системе без учета требований по защите информации;
- вероятностью нарушения надежности распространения приобретенных или созданных полезных знаний о системе без учета требований по защите информации.

В свою очередь надежное распространение приобретенных или созданных полезных знаний о системе предполагает их своевременное применение.

Обобщенный риск учитывает все вышеперечисленные вероятности соответствующих событий.

В.2.2 Оценка нарушения надежности реализации процесса

В.2.2.1 Общие положения

Для приобретения знаний о системе используют процесс приобретения. Поэтому для оценки нарушения надежности реализации процесса приобретения знаний о системе используют методы системного анализа ГОСТ Р 59329—2021 (приложение В) для оценки:

- риска незавершенности выполнения необходимых действий по поставке приобретаемых знаний;
- риска нарушения сроков поставки приобретаемых знаний;
- риска наличия недопустимого брака в приобретаемых знаниях (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций).

Соответствующие риски характеризуют вероятностью незавершения выполнения необходимых действий процесса приобретения знаний о системе, вероятностью нарушения сроков поставки приобретаемых знаний, вероятностью наличия недопустимого брака в приобретаемых знаниях в сопоставлении с возможными ущербами.

При оценке рисков расчетным вероятностным показателям сопоставляют возможный ущерб, оцениваемый тяжестью последствий для системы и ее заинтересованных сторон по договорным условиям поставки приобретаемых знаний или сравнением с подобными поставками для систем-аналогов.

В.2.2.2 Оценка незавершенности выполнения необходимых действий процесса

В каждом процессе приобретения знаний о системе должны быть выполнены необходимые действия. Незавершение необходимых действий процесса — это угроза возможного ущерба. С точки зрения тяжести ущерба в случае незавершения выполнения необходимых действий процесса приобретаемые знания могут быть условно сгруппированы по K типам, $K \geq 1$. В общем случае для каждого типа требования к завершенности процесса приобретения знаний формулируют на уровне инструкций должностных лиц, участвующих в реализации процесса.

При оценке риска вычисляют вероятность незавершения выполнения необходимых действий, связанных с приобретением по отдельной группе знаний или по всему множеству типов приобретаемых знаний. На основе применения статистических данных вероятность незавершения выполнения необходимых действий процесса для знаний k-го типа за задаваемое время $T_{\text{зад}\,k}$ вычисляют по формуле

$$R_{\text{действий}\,k}(T_{\text{зад}\,k}) = G_{\text{наруш}\,k}(T_{\text{зад}\,k})/G_k(T_{\text{зад}\,k}), \quad \text{(В.2)}$$

где $G_{\text{наруш}\,k}(T_{\text{зад}\,k})$ и $G_k(T_{\text{зад}\,k})$ — соответственно количество случаев незавершения выполнения необходимых действий процесса и общее количество необходимых действий процесса, подлежащих выполнению за заданное время $T_{\text{зад}\,k}$ для знаний k-го типа согласно статистическим данным.

Показатель завершенности выполнения необходимых действий для знаний k-го типа $Z_{\text{действий}\,k}(T_{\text{зад}\,k})$ определен следующим образом:

$$Z_{\text{действий}\,k}(T_{\text{зад}\,k}) = \begin{cases} 0, \text{ если условия завершения необходимых действий выполнены;} \\ R_{\text{действий}\,k}(T_{\text{зад}\,k}) \text{ по (В.2), если условия не выполнены или не заданы.} \end{cases} \quad \text{(В.3)}$$

Условие завершения необходимых действий по знаниям k-го типа определено как условие непревышения максимально допустимого уровня $R_{\text{доп.действий}\,k}(T_{\text{зад}\,k})$, задаваемого для вероятности незавершения выполнения необходимых действий приобретения по знаниям k-го типа. Это условие выражается в форме: $R_{\text{действий}\,k}(T_{\text{зад}\,k}) \leq R_{\text{доп.действий}\,k}(T_{\text{зад}\,k})$. В выражении для обобщенного риска показатель завершенности выполнения необходимых действий для процесса приобретения знаний k-го типа $Z_{\text{действий}\,k}(T_{\text{зад}\,k})$ обозначен как $Z(\text{пр})_{\text{действий}\,k}(T_{\text{зад}\,k})$ — см. выражение (В.14).

Вероятность незавершения выполнения необходимых действий приобретения по всему множеству знаний различных типов согласно статистическим данным вычисляют по формуле

$$R_{\text{действий}}\left(T_{\text{зад}}\right) = 1 - \sum_{k=1}^{K} W_k \left[1 - R_{\text{действий}\,k}\left(T_{\text{зад}\,k}\right)\right] / \sum_{k=1}^{K} W_k, \quad \text{(В.4)}$$

где $T_{\text{зад}}$ — задаваемое суммарное время на реализацию процесса для всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад}\,k}$ с учетом их наложений;

W_k — количество учитываемых поставок приобретаемых знаний k-го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $W(\text{пр})_k$, $k = 1, \ldots, K(\text{пр})$ — см. выражение (В.14).

В.2.2.3 Оценка нарушения сроков поставки приобретаемых знаний

В.2.2.3.1 Каждый процесс приобретения знаний должен быть выполнен в задаваемые сроки. Нарушение сроков поставки — это угроза возможного ущерба. С точки зрения важности и срочности приобретаемых знаний и тяжести ущерба в случае нарушения сроков поставки приобретаемые знания могут быть условно сгруппированы по I типам, $I \geq 1$. В общем случае для каждого типа требования к своевременности поставки приобретаемых знаний формулируют в виде: срок поставки знаний i-го типа должен быть не более задаваемого $T_{\text{зад}\,i}$, $i = 1, \ldots, I$. Неприемлемость нарушения задаваемых сроков поставки фиксируют в договорных условиях в виде штрафных санкций для поставщика, особых условий страхования ответственности и иных обязательств, направленных на недопущение нарушений сроков поставки знаний.

В.2.2.3.2 При оценке риска вычисляют вероятность нарушения сроков однократной и множественных поставок для разнородных знаний.

На основе применения статистических данных вероятность нарушения сроков однократной поставки для знаний i-го типа за задаваемое время $T_{\text{зад}\,i}$ определяют по формуле

$$R_{\text{св}\,i}(T_{\text{зад}\,i}) = N_{\text{наруш}\,i}(T_{\text{зад}\,i}) / N_i(T_{\text{зад}\,i}), \quad \text{(В.5)}$$

где $N_{\text{наруш}\,i}(T_{\text{зад}\,i})$ и $N_i(T_{\text{зад}\,i})$ — соответственно количество нарушений сроков поставки и общее количество поставок за заданное время $T_{\text{зад}\,i}$ для знаний i-го типа согласно статистическим данным

Показатель выполнения сроков поставки для знаний k-го типа определен следующим образом:

$$Z_{\text{срок}\,i}\left(T_{\text{зад}\,i}\right) = \begin{cases} 0, \text{ если условия сроков поставки выполнены;} \\ R_{\text{св}\,i}\left(T_{\text{зад}\,i}\right) \text{ по (В.5), если условия не выполнены или не заданы.} \end{cases} \quad \text{(В.6)}$$

Условие выполнения сроков поставки знаний k-го типа определено как условие непревышения максимально допустимого уровня $R_{\text{доп.св}\,i}(T_{\text{зад}\,i})$, задаваемого для вероятности нарушения сроков однократной поставки. Это условие выражается в форме: $R_{\text{св}\,i}(T_{\text{зад}\,i}) \leq R_{\text{доп.св}\,i}(T_{\text{зад}\,i})$. В выражении для обобщенного риска показатель выполнения сроков поставки для процесса приобретения знаний i-го типа $Z_{\text{срок}\,i}(T_{\text{зад}\,i})$ обозначен как $Z(\text{пр})_{\text{срок}\,i}(T_{\text{зад}\,i})$ — см. выражение (В.14).

Вероятность нарушения сроков поставки по всему множеству знаний различных типов, реализуемых в процессе согласно статистическим данным с учетом множественности поставок, характеризуемых исходными данными по каждому из типов знаний, определяют по формуле

$$R_{\text{св}}(T_{\text{зад}}) = 1 - \sum_{i=1}^{I} M_i \left[1 - R_{\text{св}\,i}(T_{\text{зад}\,i})\right] / \sum_{i=1}^{I} M_i. \quad \text{(В.7)}$$

Здесь $T_{\text{зад}}$ — задаваемое суммарное время поставки всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад}\,i}$ с учетом их наложений, M_i — количество учитываемых поставок знаний i-го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $M(\text{пр})_i$, $i = 1, \ldots, I(\text{пр})$ — см. выражение (В.14).

В.2.2.4 Оценка наличия недопустимого брака в приобретаемых знаниях

В.2.2.4.1 При реализации каждого процесса приобретаемые знания должны удовлетворять требованиям по качеству. Наличие недопустимого брака (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций) в приобретаемых знаниях — это угроза возможного ущерба. В общем случае под выполнением требований по качеству понимается поставка знаний без брака или с допустимым уровнем брака, оговоренным в договорных условиях. С точки зрения нарушения качества приобретаемых знаний и тяжести возможного ущерба приобретаемые знания могут быть условно сгруппированы по J типам, $J \geq 1$.

Неприемлемость нарушений задаваемых ограничений фиксируют в договорных условиях в виде штрафных санкций для поставщика знаний, особых условий страхования ответственности и иных обязательств, направленных на недопущение брака.

В.2.2.4.2 При оценке риска вычисляют вероятность наличия брака при однократной и множественных поставках разнородных знаний.

На основе применения статистических данных вероятность наличия брака при однократной поставке знаний j-го типа за задаваемое время $T_{зад\,j}$ определяют по формуле

$$R_{брака\,j}(T_{зад\,j}) = N_{наруш\,j}(T_{зад\,j}) / N_j(T_{зад\,j}), \quad (В.8)$$

где $N_{наруш\,j}(T_{зад\,j})$ и $N(T_{зад\,j})$ — соответственно количество поставок с недопустимым браком и общее количество поставок за заданное время $T_{зад\,j}$ для знаний j-го типа согласно статистическим данным.

Показатель отсутствия брака в поставке знаний j-го типа определен следующим образом:

$$Z_{брака\,j}(T_{зад\,j}) = \begin{cases} 0, \text{ если условия по отсутствию брака в поставке выполнены;} \\ R_{брака\,j}(T_{зад\,j}) \text{ по (В.8), если условия не выполнены или не заданы.} \end{cases} \quad (В.9)$$

Условие отсутствия брака в приобретаемых знаниях k-го типа определено как условие непревышения максимально допустимого уровня $R_{доп.брака\,j}(T_{зад\,j})$, задаваемого для вероятности наличия брака в поставке. Это условие выражается в форме: $R_{брака\,j}(T_{зад\,j}) \le R_{доп.брака\,j}(T_{зад\,j})$. В выражении для обобщенного риска показатель отсутствия брака для процесса приобретения знаний j-го типа $Z_{брака\,j}(T_{зад\,j})$ обозначен как $Z(пр)_{брака\,j}(T_{зад\,j})$ — см. выражение (В.14).

Вероятность наличия брака по всему множеству знаний различных типов, реализуемых согласно статистическим данным с учетом множественности поставок и характеризуемых исходными данными по каждому из типов знаний, вычисляют по формуле

$$R_{брака}(T_{зад}) = 1 - \sum_{j=1}^{J} L_j \left[1 - R_{брака\,j}(T_{зад\,j})\right] / \sum_{j=1}^{J} L_j \ , \quad (В.10)$$

где $T_{зад}$ — задаваемое суммарное время поставки всего множества знаний различных типов, включающее в себя все частные значения $T_{зад\,j}$ с учетом их наложений;

L_j — количество учитываемых поставок знаний j-го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение $L(пр)_j$, $j = 1, \ldots, J(пр)$ — см. выражение (В.14).

В.2.3 Оценка нарушения надежности создания полезных знаний о системе

В.2.3.1 Общие положения

Для оценки надежности создания полезных знаний о системе без учета требований по защите информации адаптируют методы системного анализа В.2.2 в части оценки:

- риска незавершенности выполнения необходимых действий по созданию знаний;
- риска нарушения сроков создания знаний;
- риска наличия недопустимого брака в создаваемых знаниях (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций).

Соответствующие риски характеризуются вероятностью незавершения выполнения необходимых действий по созданию знаний, вероятностью нарушения сроков поставки создаваемых знаний, вероятностью наличия недопустимого брака в создаваемых знаниях в сопоставлении с возможным ущербом.

В общем случае выполнение или невыполнение договорных условий по созданию знаний отслеживается с использованием индикаторной функции $Ind(\alpha)$, которая позволяет учесть последствия, связанные с нарушениями заданных условий согласно собираемой статистике для выделяемых типов знаний, — см. выражения (В.3), (В.6), (В.9).

При оценке рисков расчетным вероятностным показателям сопоставляют возможный ущерб, оцениваемый тяжестью последствий для системы и ее заинтересованных сторон.

В.2.3.2 Оценка незавершенности выполнения необходимых действий по созданию знаний

В.2.3.2.1 Настоящие оценки аналогичны оценкам по В.2.3.1. В процессе управления знаниями о системе могут быть выполнены необходимые действия по созданию знаний. Незавершение необходимых действий по созданию знаний — это угроза возможного ущерба. С точки зрения тяжести ущерба в случае незавершения выполнения необходимых действий создаваемые знания могут быть условно сгруппированы по K типам, $K \ge 1$. В общем случае для каждого типа требования к завершенности действий по созданию знаний формулируют на уровне инструкций должностных лиц, участвующих в реализации процесса.

В.2.3.2.2 При оценке риска вычисляют вероятность незавершения выполнения необходимых действий по созданию знаний по отдельной группе знаний или по всему множеству типов создаваемых знаний.

На основе применения статистических данных вероятность незавершения выполнения необходимых действий процесса для знаний k-го типа за задаваемое время $T_{зад\,k}$ вычисляют по формуле (В.2), где $G_{наруш\,k}(T_{зад\,k})$ и $G_k(T_{зад\,k})$ — соответственно количество случаев незавершения выполнения необходимых действий процесса и общее количество необходимых действий по созданию знаний, подлежащих выполнению за заданное время $T_{зад\,k}$ для знаний k-го типа согласно статистическим данным.

Показатель завершенности выполнения необходимых действий при создании знаний k-го типа определен выражением (В.3). При этом в выражении для обобщенного риска показатель завершенности выполнения необходимых действий по созданию знаний k-го типа $Z_{\text{действий } k}(T_{\text{зад } k})$ обозначен как $Z(\text{созд})_{\text{действий } k}(T_{\text{зад } k})$ — см. выражение (В.14).

Вероятность незавершения выполнения необходимых действий процесса по всему множеству знаний различных типов согласно статистическим данным определяют по адаптируемой формуле (В.4).

При адаптации используемые в формуле (В.4) исходные данные означают:

$T_{\text{зад}}$ — задаваемое суммарное время на реализацию процесса для всего множества создаваемых знаний различных типов, включающее в себя все частные значения $T_{\text{зад } k}$ с учетом их наложений;

W_k — количество учитываемых случаев создания знаний k-го типа при множественных поставках знаний, в выражении для обобщенного риска применительно к действиям по созданию знаний использовано обозначение $W(\text{созд})_k$, $k = 1, \ldots, K(\text{созд})$ — см. выражение (В.14).

В.2.3.3 Оценка нарушения сроков создания знаний

В.2.3.3.1 Создание знаний в процессе управления знаниями о системе должно быть выполнено в задаваемые сроки. Нарушение сроков создания знаний — это угроза возможного ущерба. С точки зрения важности и срочности создания знаний и тяжести ущерба в случае нарушения сроков создаваемые знания могут быть условно сгруппированы по I типам, $I \geq 1$. В общем случае для каждого типа требования к своевременности создания знаний формулируют в виде: срок создания знаний i-го типа должен быть не более задаваемого $T_{\text{зад } i}$, $i = 1, \ldots, I$. Неприемлемость нарушения задаваемых сроков создания знаний фиксируют в договорных условиях в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение нарушений установленных сроков.

В.2.3.3.2 При оценке риска вычисляют вероятность нарушения сроков, задаваемых в случаях однократного и множественного создания разнородных знаний.

На основе применения статистических данных вероятность нарушения сроков однократного создания знаний i-го типа за задаваемое время $T_{\text{зад } i}$ вычисляют по формуле (В.5), где $N_{\text{наруш } i}(T_{\text{зад } i})$ и $N_i(T_{\text{зад } i})$ — соответственно количество нарушений сроков создания и общее количество заказов на создание знаний за заданное время $T_{\text{зад } i}$ для знаний i-го типа согласно статистическим данным.

Показатель выполнения сроков создания знаний k-го типа определен выражением (В.6). В выражении для обобщенного риска показатель выполнения сроков создания знаний i-го типа $Z_{\text{срок } i}(T_{\text{зад } i})$ обозначен как $Z(\text{созд})_{\text{срок } i}(T_{\text{зад } i})$ — см. выражение (В.14).

Вероятность нарушения сроков создания по всему множеству знаний различных типов, реализуемых согласно статистическим данным, вычисляют по адаптируемой формуле (В.7). При адаптации используемые в формуле (В.7) исходные данные означают: $T_{\text{зад}}$ — задаваемое суммарное время создания всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад } i}$ с учетом их наложений, M_i — это количество учитываемых случаев создания знаний i-го типа при множественных знаниях, в выражении для обобщенного риска применительно к процессу создания использовано обозначение $M(\text{созд})_i$, $i = 1, \ldots, I(\text{созд})$ — см. выражение (В.14).

В.2.3.4 Оценка наличия недопустимого брака в создаваемых знаниях

В.2.3.4.1 Создаваемые знания должны удовлетворять требованиям по качеству. Наличие недопустимого брака (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций) в создаваемых знаниях — это угроза возможного ущерба. В общем случае под выполнением требований по качеству понимается создание знаний без брака или с допустимым уровнем брака, оговоренным в договорных условиях. С точки зрения нарушения качества создаваемых знаний и тяжести возможного ущерба знания могут быть условно сгруппированы по J типам, $J \geq 1$.

Неприемлемость нарушений задаваемых ограничений фиксируют в договорных условиях в виде штрафных санкций для организаций, создающих знания, особых условий страхования ответственности и иных обязательств, направленных на недопущение брака.

В.2.3.4.2 При оценке риска вычисляют вероятность наличия брака в случаях однократного и множественного создания разнородных знаний.

На основе применения статистических данных вероятность наличия брака при однократном создании знаний j-го типа за задаваемое время $T_{\text{зад } j}$ определяют по формуле (В.8), где $N_{\text{наруш } j}(T_{\text{зад } j})$ и $N(T_{\text{зад } j})$ — соответственно количество случаев создания знаний с недопустимым браком и общее количество созданных знаний j-го типа за заданное время $T_{\text{зад } j}$ согласно статистическим данным.

Показатель отсутствия брака в создаваемых знаниях j-го типа определен выражением (В.9).

Вероятность наличия брака по всему множеству знаний различных типов, реализуемых согласно статистическим данным, вычисляют по адаптируемой формуле (В.10). При адаптации используемые в формуле (В.10) исходные данные означают: $T_{\text{зад}}$ — задаваемое суммарное время создания всего множества знаний различных типов, включающее в себя все частные значения $T_{\text{зад } j}$ с учетом их наложений. L_j — это количество учитываемых случаев создания активов знаний j-го типа при множественных случаях создания, в выражении для обобщенного риска применительно к созданию знаний использовано обозначение $L(\text{созд})_j$, $j = 1, \ldots, J(\text{созд})$ — см. выражение (В.14).

В.2.4 Модель для оценки вероятности нарушения надежности распространения полезных знаний

Модель позволяет оценить вероятность $R_{\text{распред}}$ нарушения надежности распространения полезных знаний (как приобретенных, так и созданных — см. В.2.2 и В.2.3) для их своевременного применения.

Примечание — В настоящей модели надежность распространения полезных знаний с доведением их до потребителей предполагает своевременность их применения.

Речь идет о знаниях, которые подлежат распространению по потребителям в условиях возможной неопределенности в сроках их приобретения или создания (в том числе обновления) и их изменяющейся полезности. Полезными признают знания о системе, приобретение и/или создание и своевременное применение которых способно в заданных условиях принести пользу системе, связанным с ней системам и/или обеспечить удовлетворенность заинтересованных сторон. Полезность знаний может естественным образом устаревать со временем, т. е. терять свою значимость для выполнения системой своих функций с требуемой эффективностью и/или безопасностью.

Надежность распространения полезных знаний обеспечивают на основе выявления значимых изменений в их полезности, реализации эффективных технологий обновления знаний в базе знаний системы, а также за счет санкционированного распространения применяемых знаний по потребителям.

При экспоненциальной аппроксимации распространений исходных характеристик и их независимости вероятность нарушения надежности распространения полезных знаний $R_{\text{распред}}$ (с сохранением полезности на момент их использования) вычисляют по формулам:

- для дисциплины распространения знаний сразу после их приобретения или создания

$$R_{\text{распред}} = 1 - \frac{\xi}{\xi + T_{\text{база знаний}}}; \tag{В.11}$$

- для дисциплины периодического распространения знаний вне зависимости от сроков их приобретения или создания, т. е. по регламенту (при отсутствии изменения полезности подтверждается полезность существующих хранимых знаний)

$$R_{\text{распред}} = 1 - \frac{\xi^2}{q(\xi + T_{\text{база знаний}})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right], \tag{В.12}$$

где ξ — среднее время между значимыми изменениями реальной полезности относительно знаний, хранимых в базе знаний системы. Значимые изменения требуют обновления существующих хранимых знаний (т. е. ξ^{-1} — частота значимого изменения полезности знаний);

$T_{\text{база знаний}}$ — среднее время приобретения или создания и помещения в базу знаний системы новых знаний (от создателей или распространителей знаний);

q — установленное регламентом время между соседними доведениями обновленных знаний до потребителей системы (т. е. q^{-1} — частота распространения обновляемых знаний для дисциплины периодического распространения знаний по регламенту).

Для периода $T_{\text{зад}}$, для которого определены исходные данные ξ, $T_{\text{база знаний}}$, q, показатель надежности распространения полезных знаний, предполагающий своевременность их последующего применения, определен следующим образом

$$Z_{\text{полезн}}(T_{\text{зад}}) = \begin{cases} 0, & \text{если условия по распространению и применению знаний выполнены;} \\ R_{\text{распред}}(T_{\text{зад}}) \text{ по (В.11)} - \text{(В.12)}, & \text{если условия не выполнены или не заданы.} \end{cases} \tag{В.13}$$

Условие по распространению и применению полезных знаний определено как условие непревышения максимально допустимого уровня $R_{\text{доп.распред}}(T_{\text{зад}})$, задаваемого для вероятности нарушения надежности распространения полезных знаний. Это условие выражается в форме: $R_{\text{распред}}(T_{\text{зад}}) \le R_{\text{доп.распред}}(T_{\text{зад}})$.

В.2.5 Оценка обобщенного риска нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации

В.2.5.1 Общие положения

Обобщенный риск нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации оценивают с использованием расчетных вероятностей нарушения надежности реализации процесса приобретения знаний (см. В.2.2), нарушения надежности создания полезных знаний о системе (см. В.2.3), нарушения надежности распространения приобретенных или созданных полезных знаний о системе (см. В.2.4).

При этом обобщенная вероятность нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации характеризуется переходом в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по причинам: из-за незавершения выполнения необходимых действий процесса либо из-за нарушения сроков поставки, либо из-за наличия недопустимого брака в приобретаемых или создаваемых знаниях, либо из-за нарушения надежности распространения полезных знаний, либо из-за комбинации каких-либо перечисленных выше причин.

В.2.5.2 Метод оценки

Обобщенную вероятность $R_{\text{обобщен}}(T_{\text{зад}})$ нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации вычисляют по формуле

$$R_{\text{обобщен}}(T_{\text{зад}}) = 1-\left[1-Z_{\text{полезн}}(T_{\text{зад}})\right]\cdot\left\{\sum_{k=1}^{K(\text{пр})} W(\text{пр})_k\left[1-Z(\text{пр})_{\text{действий}\,k}(T_{\text{зад}\,k})\right]+\right.$$
$$+\sum_{k=1}^{K(\text{созд})} W(\text{созд})_k\left[1-Z(\text{созд})_{\text{действий}\,k}(T_{\text{зад}\,k})\right]+\sum_{i=1}^{I(\text{пр})} M(\text{пр})_i\left[1-Z(\text{пр})_{\text{срок}\,i}(T_{\text{зад}\,i})\right]+$$
$$+\sum_{i=1}^{I(\text{созд})} M(\text{созд})_i\left[1-Z(\text{созд})_{\text{срок}\,i}(T_{\text{зад}\,i})\right]+\sum_{j=1}^{J(\text{пр})} L(\text{пр})_j\left[1-Z(\text{пр})_{\text{брака}\,j}(T_{\text{зад}\,j})\right]+ \qquad \text{(В.14)}$$
$$\left.+\sum_{j=1}^{J(\text{созд})} L(\text{созд})_j\left[1-Z(\text{созд})_{\text{брака}\,j}(T_{\text{зад}\,j})\right]\right\}/\left[\sum_{k=1}^{K(\text{пр})} W(\text{пр})_k+\sum_{i=1}^{I(\text{пр})} M(\text{пр})_i+\sum_{j=1}^{J(\text{пр})} L(\text{пр})_j+\right.$$
$$\left.+\sum_{k=1}^{K(\text{созд})} W(\text{созд})_k+\sum_{i=1}^{I(\text{созд})} M(\text{созд})_j+\sum_{j=1}^{J(\text{созд})} L(\text{созд})_j\right],$$

где $T_{\text{зад}}$ — задаваемое суммарное время, включающее в себя все частные значения $T_{\text{зад}\,k}$, $T_{\text{зад}\,i}$, $T_{\text{зад}\,j}$ с учетом их наложений, — см. формулы (В.2) — (В.13).

Остальные исходные данные определены в В.2.2 — В.2.4.

Если все условия по завершению необходимых действий процесса управления знаниями о системе, выполнению сроков поставки знаний, отсутствию брака в поставке приобретаемых и создаваемых знаний, распространению и применению полезных знаний выполнены, то вероятность нарушения надежности реализации процесса управления знаниями о системе без учета требований по защите информации обращается в ноль.

В.3 Модели для прогнозирования риска нарушения требований по защите информации (включая сохранение знаний)

В.3.1 Общие положения

В.3.1.1 Прогнозирование риска нарушения требований по защите информации осуществляют на основе применения математических моделей для прогнозирования риска нарушения требований по защите информации из ГОСТ Р 59341—2021 (В.2). Все положения по моделированию, изложенные в ГОСТ Р 59341 применительно к процессу управления информацией, в полной мере применимы к процессу управления знаниями о системе (в части, свойственной прогнозированию риска нарушения требований по защите информации). Для расчета типовых показателей рисков анализируемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. В моделях и методах системного анализа применительно к таким моделируемым системам используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики по процессу и возможным условиям его реализации.

В.3.1.2 В моделях простой структуры под анализируемой системой понимают определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявлены требования и выполняют меры защиты информации. Система простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединенных для анализа как один элемент. Анализ системы простой структуры осуществляют по принципу «черного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы. Система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых представляется в виде «черного ящика», функционирующего в условиях неопределенности.

В.3.1.3 При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если…», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.3.1.4 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается целостность моделируемой системы, включая изначальное выполнение требований по защите информации в системе (в качестве моделируемой системы простой или сложной структуры могут быть рассмотрены, например, выходные результаты с задействованными активами или действия процесса, к которым предъявлены определенные требования по защите информации);
- в условиях неопределенностей возникновение и разрастание различных угроз безопасности информации описывается в терминах случайных событий;

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

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

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

- «Выполнение требований по защите информации в системе нарушено» — в противном случае.

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение успешной реализации процесса управления знаниями о системе.

В.3.1.5 В моделях простой структуры систему рассматривают как «черный ящик», если для него сделано предположение об использовании одной и той же модели угроз безопасности информации и одной и той же технологии системного контроля выполнения требований по защите информации и восстановления системы после состоявшихся нарушений или выявленных предпосылок к нарушениям. В моделях сложной структуры под моделируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логически представляет собой определенное действие или выходной результат и совокупность задействованных активов, к которым предъявлены требования и применяют меры защиты информации. При этом выходной результат сам может стать активом в итоге выполняемых действий.

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

В.3.1.6 При расчетах с использованием математических моделей для прогнозирования риска нарушения требований по защите информации и рекомендаций ГОСТ Р 59341—2021 (В.2, В.3 приложения В) осуществляют учет предпринимаемых мер периодической диагностики и восстановления возможностей по обеспечению выполнения требований по защите информации. В результате математического моделирования рассчитывают вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение до единицы, представляющее собой вероятность нарушения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе нарушено»). В свою очередь вероятность нарушения требований по защите информации в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения требований по защите информации в процессе управления знаниями о системе.

В.3.2 Исходные данные и расчетные показатели

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

σ — частота возникновения источников угроз в процессе управления знаниями о системе;

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

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

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

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

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

Расчетные показатели:

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

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

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

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

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

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

$$R_{интегр}\left(T_{зад}\right)=1-\left[1-R_{обобщен}\left(T_{зад}\right)\right]\cdot\left[1-R_{наруш}(T_{зад})\right], \quad (В.15)$$

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

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

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса управления знаниями о системе

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

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

При этом риски характеризуют прогнозными вероятностными значениями в сопоставлении с возможными оценками ущербов.

Расчетные значения рисков на заданный период прогноза используют для решения задач системного анализа (см. раздел 7).

Примечание — Оценка ущербов не входит в состав настоящих методических указаний. Для разработки самостоятельной методики по оценке ущербов согласно приложению Е учитывают специфику систем — см., например ГОСТ Р 22.10.01, ГОСТ Р 54145. При этом должны учитываться соответствующие положения законодательства Российской Федерации [1] — [15].

Г.1 Анализируемые объекты для прогнозирования рисков

Применительно к конкретной системе для прогнозирования рисков согласно 5.3, 6.3 определению подлежат:

- состав выходных результатов и выполняемых действий процесса управления знаниями о системе и используемых при этом активов;
- перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для выходных результатов, выполняемых действий процесса управления знаниями о системе и используемых при этом активов;
- технологии противодействия угрозам, используемые в процессе управления знаниями о системе в заданной среде применения системы;
- формализованные требования или условия по завершению необходимых действий процесса управления знаниями о системе, соблюдению сроков поставки знаний, отсутствию брака в приобретаемых и создаваемых знаниях, распространению и применению полезных знаний о системе.

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

В зависимости от целей прогнозирования рисков модели и методы, рекомендуемые в приложении В, относятся к моделям, представляемым 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 (системного элемента) в течение задаваемого периода прогноза означает такое состояние этой системы (системного элемента), которое в течение этого периода прогноза отвечает целевому назначению применяемой модели.

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 Логическое 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 управления знаниями о системе 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.

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

Г.3 Положения по формализации

Для решения задач системного анализа в качестве моделируемой системы могут выступать: множество выходных результатов и активов, множество действий процесса управления знаниями о системе, объединенных целевым назначением в рассматриваемой системе.

Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи системного анализа. В общем случае моделируемую систему представляют в виде «черного ящика» либо в виде сложной системы, элементы которой объединяются последовательно или параллельно. Примеры декомпозиции сложной системы до составных элементов представлены на рисунках Г.1, Г.2. При этом для каждого элемента могут оказаться характерными свои разнородные угрозы и применяемые технологии 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)

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

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

- «Выполнение требований по защите информации в процессе управления знаниями о системе обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации, т. е. с точки зрения математического моделирования их невыполнение ведет к ущербу;
- «Выполнение требований по защите информации в процессе управления знаниями о системе нарушено» — в противном случае.

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

- «Надежность реализации процесса управления знаниями о системе и выполнение требований по защите информации в системе обеспечены», если в течение всего периода прогноза обеспечены и надежность выполнения определенных действий процесса для получения выходных результатов, и выполнение определенных требований по защите информации;
- «Надежность реализации процесса управления знаниями о системе и/или выполнение требований по защите информации в системе нарушено» — в противном случае.

В общем случае возможно расширение или переименование самих элементарных состояний, главное, чтобы они формировали полное множество аналогично множествам, введенным в настоящем подразделе. В Г.7.2—Г.7.4 приведены примеры прогнозирования рисков.

Использование аппарата прогнозирования рисков позволяет обосновывать допустимые риски. По существу, для каждого анализируемого объекта существуют свои условия приемлемости в использовании по назначению. Приоритетным является выбор критерия допустимого риска, основанного на прецедентном принципе — см. ГОСТ Р 59349.

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 (системы, процесса, системного элемента). При использовании задаваемых границ допустимого риска прогнозы для реальных случаев нарушений нормы «до» и «после» наступления нарушений позволяют (при использовании задаваемых количественно границ допустимого риска) выполнить аналитическое обоснование 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 и действий, предупреждающих возникновение ущербов при ограничениях на ресурсы и допустимые риски, а также оценка и обоснование эффективных кратко-, средне- и долгосрочных планов по обеспечению безопасности осуществляют путем решения самостоятельных оптимизационных задач, использующих расчетные значения прогнозируемых рисков (см. рекомендуемый перечень методик в приложении Е).

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

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

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

Г.4 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе, которая может быть представлена в виде «черного ящика» (см. В.2, В.4) или сложной логической структуры (см. В.3), расчетными показателями являются:

$R_{обобщен}(T_{зад})$ — риск нарушения надежности реализации процесса управления знаниями о системе в течение задаваемого периода прогноза $T_{зад}$ без учета требований по защите информации;

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

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

Применительно к моделируемой системе исходными являются данные, необходимые для проведения расчетов по моделям В.2, В.3. Расчеты осуществляют по рекомендациям В.2—В.4.

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

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

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

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

Шаг 4. Выбирают расчетные показатели и подходящие математические модели и методы (включая методы повышения их адекватности). Осуществляют расчет выбранных показателей с использованием расчетных соотношений (В.1) — (В.15). Действия осуществляют согласно Г.4.

Г.6 Обработка и использование результатов прогнозирования

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

Г.7 Примеры

Г.7.1 Нижеследующие примеры призваны продемонстрировать отдельные аналитические возможности методов и моделей настоящего стандарта.

Согласно [27] для достижения основных целей государственной политики Российской Федерации в Арктике на период до 2035 года должны быть системно решены многочисленные задачи в сферах социального и экономического развития, развития инфраструктуры Арктической зоны, развития науки и технологий в интересах освоения Арктики, охраны окружающей среды и обеспечения экологической безопасности, развития международного сотрудничества, обеспечения защиты населения и территорий Арктической зоны Российской Федерации от чрезвычайных ситуаций природного и техногенного характера, обеспечения общественной и военной безопасности, защиты и охраны государственной границы Российской Федерации. Системное решение всего множества задач основано на управлении знаниями, базирующемся на аналитической обработке разнородных

данных мониторинга и предусматривающем совершенствование, накопление и своевременное применение появляющихся знаний, — см. рисунок Г.3. Неизбежные неопределенности в специфике приложений для заданного периода прогноза (с начальной точки t_1 до момента t_x в будущем) учитывают при решении практических задач с использованием математического моделирования, прогнозирования рисков, системного анализа и оптимизации на различных метауровнях.

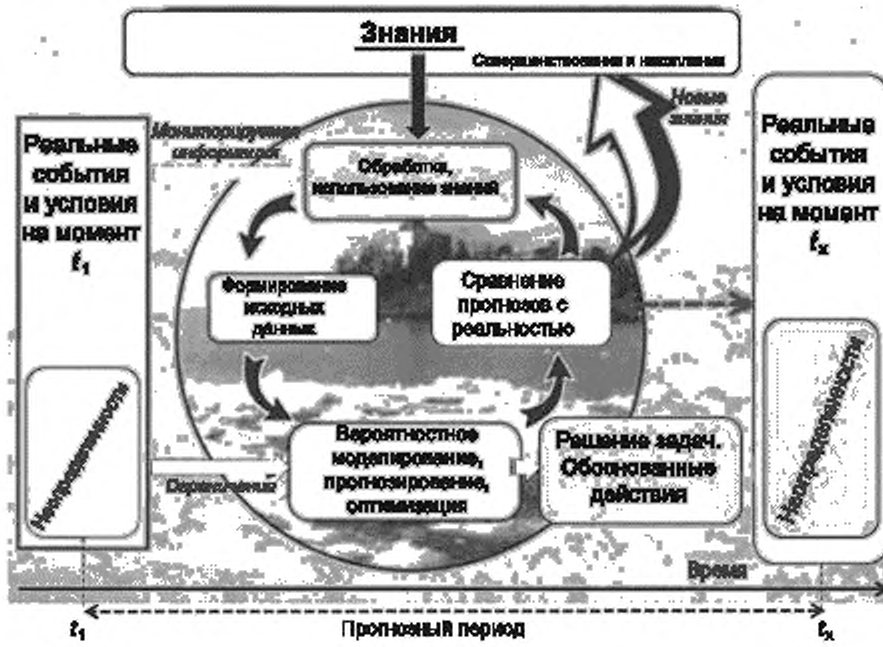


Рисунок Г.3 — Прогнозирование в управлении знаниями

Учитывая сложность и многогранность решаемых практических задач по освоению Арктики и стремление к эффективной реализации государственной политики Российской Федерации, в Арктике на период до 2035 года и последующие десятилетия создание одного или нескольких ЦЗн является неизбежным. В условиях реальных и потенциальных угроз нарушения безопасности критической информационной инфраструктуры [15] защита информации в ЦЗн имеет приоритетное значение. Не вдаваясь в детали и специфику разнородных знаний, подлежащих интеграции и применению, в рамках примеров продемонстрированы отдельные практические подходы к использованию настоящей методики:

- для решения профильных задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях (профильные задачи 1-го типа);

- для решения профильных задач обеспечения комплексной безопасности работ на континентальном шельфе, включая мониторинг и прогнозирование экстремальных ситуаций природного и техногенного характера (профильные задачи 2-го типа);

- для решения профильных задач предотвращения и ликвидации аварийных разливов нефти в ледовых условиях, включая создание технологий обнаружения нефти подо льдом (профильные задачи 3-го типа);

- для решения профильных задач разработки технологий комплексного гидрометеорологического и экологического мониторинга опасных природных явлений в арктических регионах (профильные задачи 4-го типа);

- для решения профильных задач разработки технологий дистанционного зондирования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды Арктики (профильные задачи 5-го типа).

Методика проиллюстрирована на примерах прогноза:

- рисков нарушения надежности реализации процесса управления знаниями без учета требований по защите информации;

- риска нарушения требований по защите информации;

- интегрального риска нарушения реализации процесса управления знаниями с учетом требований по защите информации.

Для определенности с точки зрения системной инженерии для эффективной защиты информации рассмотрены два варианта: создания и функционирования пяти автономных профильных ЦЗн, каждый из которых специализируется на решении своих профильных задач (вариант 1), и добавления единого ЦЗн, интегрирующего возможности всех автономных ЦЗн (вариант 2). С учетом возможных ущербов цели прогнозирования рисков сформулированы следующим образом. В условиях существующей неопределенности:

- количественно оценить риски нарушения надежности реализации процесса управления знаниями без учета требований по защите информации;
- количественно оценить риск нарушения требований по защите информации (как поэлементно за каждый ЦЗн, так и за комплекс всех ЦЗн);
- определить критичные условия в развитии различных угроз;
- количественно оценить риски нарушения надежности реализации процесса управления знаниями с учетом требований по защите информации;
- определить такой период, при котором сохраняются гарантии непревышения допустимых рисков.

Тем самым выполнены шаги 1—2 настоящей методики.

Г.7.2 Примеры 1—4 иллюстрируют оценку рисков нарушения надежности реализации процесса управления знаниями согласно рекомендациям ГОСТ Р 57133 (без учета требований по защите информации) и 6.1.3. Полагая соизмеримость возможных ущербов, в примерах оцениваются вероятности нарушения надежности реализации процесса приобретения и создания полезных знаний и вероятность нарушения надежности распространения приобретенных или созданных полезных знаний и своевременного их применения.

Г.7.2.1 Пример 1 иллюстрирует оценку рисков нарушения надежности реализации процесса приобретения знаний.

При оценке рисков нарушения надежности реализации процесса приобретения знаний адаптируют методы системного анализа ГОСТ Р 59329—2021 (приложение В) в части оценки:

- риска незавершенности выполнения необходимых действий по поставке приобретаемых знаний;
- риска нарушения сроков поставки приобретаемых знаний;
- риска наличия недопустимого брака в приобретаемых знаниях (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций).

С точки зрения расчетов, модели для оценки вышеперечисленных рисков являются идентичными, так как при оценке каждого из рисков расчетные вероятностные показатели сопоставляются с возможный ущербом, полученным из-за невыполнения условий приобретения знаний.

Ниже в примере показана оценка нарушения надежности сроков поставки приобретаемых знаний. Оценка незавершенности выполнения необходимых действий по поставке приобретаемых знаний и наличия недопустимого брака в приобретаемых знаниях (аналитических ошибок, описок, необоснованных заключений и/или рекомендаций) делается по аналогии.

Оценка риска нарушения надежности сроков поставки приобретаемых знаний осуществляется с использованием расчетных соотношений (В.5) — (В.7) согласно рекомендациям В.2.2.3.

В соответствии с поставленными задачами по развитию Арктики предполагается приобретение нескольких видов знаний i-го типа. Приобретение всех видов знаний за исключением одного проходит без нарушения сроков поставки, т. е. в этом случае $Z_{\text{срок }i}(T_{\text{зад}}) = 0$. Следовательно, при оценке риска учитывается только вид приобретаемых знаний, для которого сроки поставки нарушены.

С учетом статистических данных по развитию Арктики для определенности условно принимается, что за заданное время $T_{\text{зад }i} = 1$ год для знаний i-го типа общее количество поставок $N_i = 100$, количество нарушений сроков поставки $N_{\text{наруш }i} = 3$, что составляет 3 % от общего количества поставок, а количество множественных поставок $M_i = 1$.

Таким образом, вероятность нарушения сроков однократной поставки для знаний i-го типа за задаваемое время $T_{\text{зад }i}$: $R_{\text{св}}(T_{\text{зад}}) = 3/100 = 0{,}03$, а вероятность нарушения сроков поставки по всему множеству знаний различных типов получается: $R_{\text{св}}(T_{\text{зад}}) = 1 - 1 \cdot (1 - 0{,}03) = 0{,}03$.

Г.7.2.2 В примере 2 без изменения сути демонстрации полагается, что результаты оценки нарушения надежности реализации процесса создания полезных знаний о системе полностью идентичны результатам примера 1, посвященного оценке нарушения надежности реализации процесса приобретения знаний (см. условия и результаты в 7.2.1).

Г.7.2.3 Пример 3 иллюстрирует оценку рисков нарушения надежности реализации процесса распространения полезных знаний согласно рекомендациям В.2.4.

Пусть с учетом статистических данных частота значимого изменения полезности знаний об условиях в Арктике, хранимых в базе знаний системы, составит не более одного изменения за десятилетие, т. е. $\xi = 10$ лет. Среднее время приобретения или создания и помещения в базу знаний системы новых знаний (от создателей или распространителей знаний) составит около трех месяцев, т. е. $T_{\text{база знаний}} = 3$ мес, что в переводе к одинаковым единицам измерения составляет 0,25 года. Доведение обновлений от центров знаний до потребителей системы осуществляется ежемесячно, т. е. $q = 1$ мес или 0,083 года. Кроме того, на вероятность нарушения надежности распространения полезных знаний накладывается ограничение сверху: эта вероятность не должна превышать максимально допустимого уровня $R_{\text{доп.распред}}(T_{\text{зад}}) = 0{,}10$.

Таким образом, оценка риска для дисциплины распространения знаний сразу после их приобретения или создания определяется по формуле (В.11): $R_{распред} = 1 – 10/(10 + 0,25) = 0,024$, а оценка риска для дисциплины периодического распространения знаний вне зависимости от сроков их приобретения или создания, т. е. по регламенту (с подтверждением полезности существующих хранимых знаний при отсутствии изменений), определяется по формуле (В.12)

$$R_{распред} = 1 – 102\cdot[1 – \exp(–0,083/10)] / 0,083 \cdot (10 + 0,25) = 0,060.$$

Так как выполнено условие непревышения максимально допустимого уровня $R_{распред}(T_{зад}) \le R_{доп.распред}(T_{зад})$, то данным показателем при дальнейших расчетах можно пренебречь, т. е. $Z_{полезн}(T_{зад}) = 0$, условия по распространению знаний выполнены, см. формулу (В.13).

Г.7.2.4 В примере 4 представлена оценка обобщенного риска нарушения надежности реализации процесса управления знаниями о системе, которая определяется по формуле (В.14).

Оценка обобщенного риска нарушения надежности реализации процесса управления знаниями о системе проводится согласно рекомендациям, приведенным в В.2.5, т. е.

$$R_{обобщен}(T_{зад}) = 1 – [1\cdot(1 – 0,03) + 1\cdot(1 – 0,03) + 1\cdot(1 – 0,03) + 1\cdot(1 – 0,03) +$$
$$+ 1\cdot(1 – 0,03) + 1\cdot(1 – 0,03)]/(1 + 1 + 1 + 1 + 1 + 1) = 0,03.$$

В итоге риск нарушения надежности реализации процесса управления знаниями о системе в прогнозируемом периоде 1 год составит приблизительно 0,03.

Г.7.3 Примеры 5 и 6 иллюстрируют прогнозирование риска нарушения требований по защите информации для сравнения эффективности защиты информации в приложении к варианту 1 нескольких автономных ЦЗн, каждый из которых специализируется на решении профильных задач (см. рисунок Г.4), и варианту 2 с добавлением единого ЦЗн, интегрирующего возможности всех автономных ЦЗн и по сути исполняющего функции резервного центра при реальных отказах, связанных в том числе с нарушениями требований по защите информации, — см. рисунок Г.5.

Именно эти две структуры определяют в примерах 5 и 6 моделируемые системы.

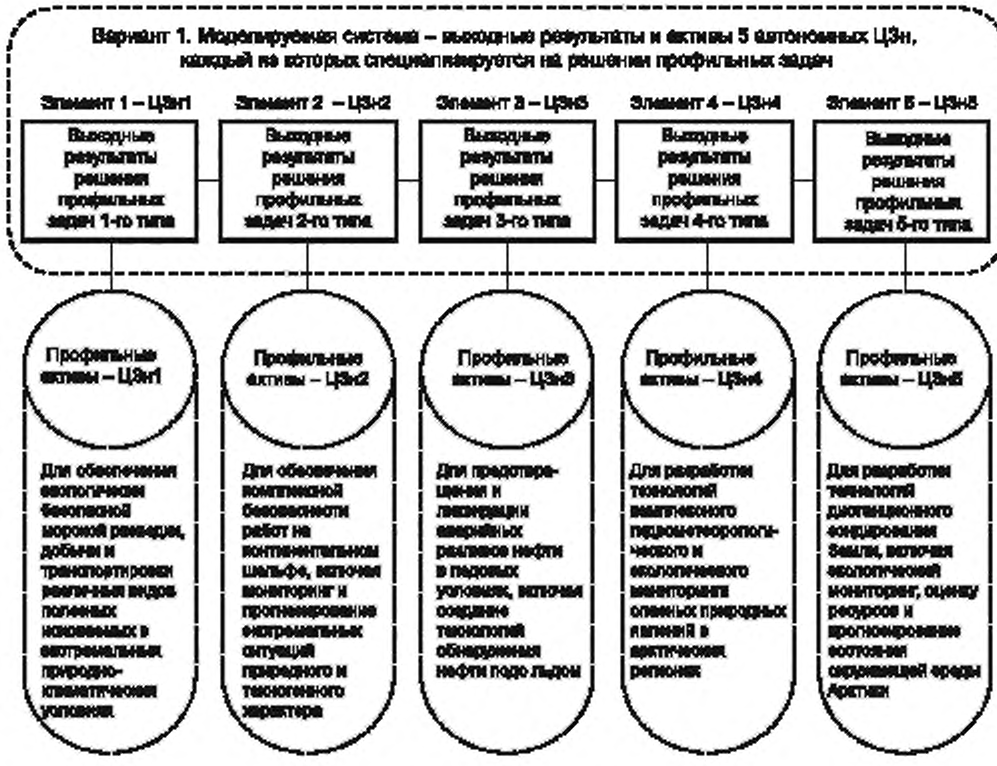


Рисунок Г.4 — Моделируемая система для варианта 1

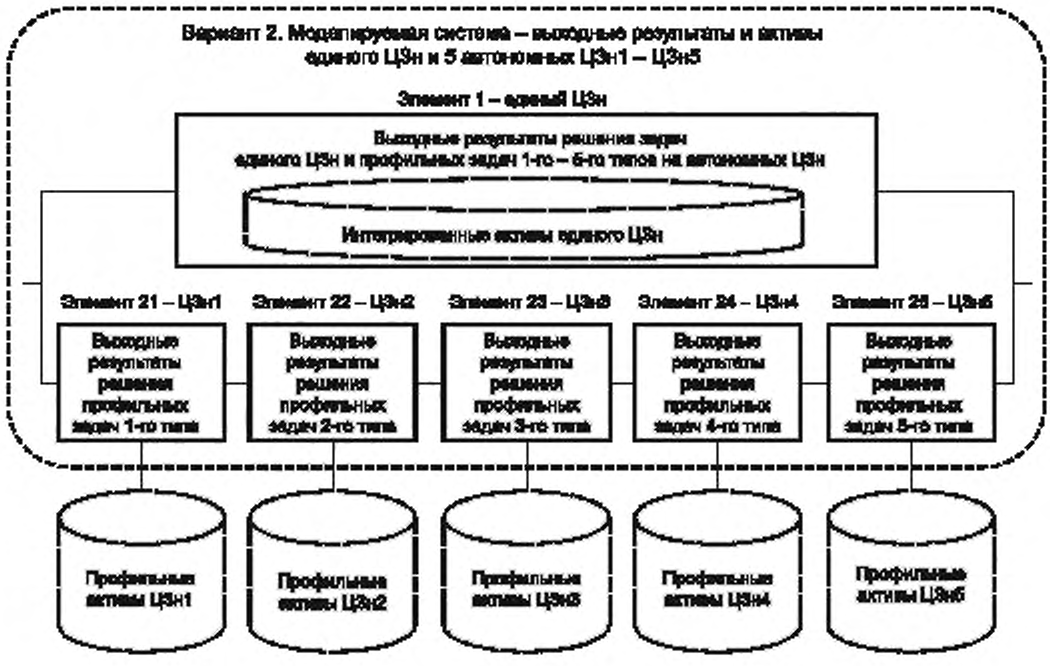


Рисунок Г.5 — Моделируемая система для варианта 2

Г.7.3.1 Пример 5 демонстрирует прогнозирование риска нарушения требований по защите информации в нескольких автономных ЦЗн (вариант 1). Элементами моделируемой системы являются элементы 1—5, формально ассоциируемые с активами и выходными результатами решения профильных задач соответственно 1-го — 5-го типов (см. рисунок Г.4).

По определению отсутствие нарушений требований по защите информации в моделируемой системе считается обеспеченным в течение заданного периода прогноза, если в течение этого периода отсутствуют нарушения во всех автономных ЦЗн. Сам период прогноза для отдельного элемента может быть интерпретирован как относящийся к стадии создания (по угрозам, свойственным этой стадии), так и к стадии эксплуатации в будущем (по потенциально возможным угрозам).

Выполняя шаг 3 методики, выявлено множество критичных угроз, влияющих на безопасность каждого из структурных элементов моделируемой системы. Гипотетичные исходные данные по каждому из пяти элементов моделируемой системы с кратким обоснованием в комментариях представлены в таблице Г.1.

Таблица Г.1 — Гипотетичные исходные данные для прогнозирования риска нарушения требований по защите информации в процессе управления знаниями о системе

Исходные данные	Элементы	Значения и комментарии
σ — частота возникновения источников угроз нарушения требований по защите информации	1	четыре раза в год, что соизмеримо с возникновением угроз, связанных с субъективными факторами и ошибками специалистов средней квалификации в области ИТ при решении задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях
	2	два раза в год, что соизмеримо со временем наработки на отказ программно-технического оборудования для обеспечения комплексной безопасности работ на континентальном шельфе, включая мониторинг и прогнозирование экстремальных ситуаций природного и техногенного характера

Продолжение таблицы Г.1

Исходные данные	Элементы	Значения и комментарии
	3	один раз в год, что соизмеримо с возникновением угроз, связанных с причинами человеческих ошибок на уровнях принятия решений по предотвращению и ликвидации аварийных разливов нефти в ледовых условиях, включая создание технологий обнаружения нефти подо льдом
	4	один раз в два года, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения в технологиях комплексного гидрометеорологического и экологического мониторинга опасных природных явлений в арктических регионах
	5	один раз в два года, что соизмеримо с возникновением угроз от использования недекларируемых возможностей программного обеспечения в технологиях дистанционного зондирования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды Арктики
β — среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации	1—5	1 сут (предполагается, что из-за источника угроз активизируются не сразу, а с некоторой задержкой не менее суток) - это время до возможного ущерба после возникновения признаков угроз
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации	1	1 ч - определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях
	2	1 ч - определяется регламентом контроля целостности программного обеспечения и активов при мониторинге экстремальных ситуаций природного и техногенного характера
	3	2 ч - определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части предотвращения и ликвидации аварийных разливов нефти в ледовых условиях
	4	1 ч - определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при комплексном гидрометеорологическом и экологическом мониторингах опасных природных явлений в арктических регионах
	5	8 ч - определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части дистанционного зондирования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды Арктики
$T_{диаг}$ — среднее время диагностики состояния активов и самой системы	1—5	30 с что соизмеримо с длительностью автоматического контроля целостности программного обеспечения и активов ЦЗн

Окончание таблицы Г.1

Исходные данные	Элементы	Значения и комментарии
$T_{восст}$ — среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений	1—5	5 мин включая перезагрузку программного обеспечения и восстановление данных ЦЗн
$T_{зад}$ — задаваемая длительность периода прогноза	1—5	от одного месяца до двух лет (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения требований по защите информации)

Выполняя шаг 4 методики, прогнозирование риска нарушения требований по защите информации осуществлено с использованием рекомендаций В.3.

Анализ результатов моделирования согласно рекомендациям В.3 показал, что в вероятностном выражении риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,222 — см. рисунок Г.6, составляя для 1-го элемента — 0,080 («узкое место»), для 2-го — 4-го элементов не превышая 0,041, а для 5-го элемента — 0,072 («узкое место»). При изменении длительности периода прогноза от одного до четырех месяцев риск возрастает от 0,020 до 0,080. Для допустимого риска на уровне 0,050 обоснован период до 2,5 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса центров знаний, характеризуемых условиями примера из таблицы Г.1, — см. рисунок Г.7.

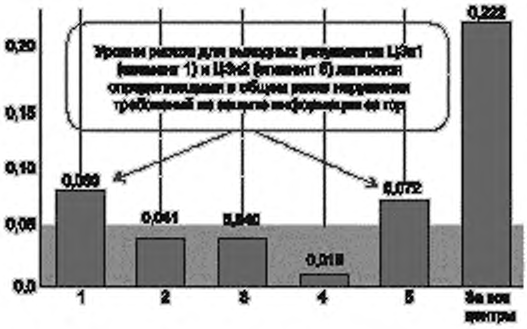


Рисунок Г.6 — Оценки риска нарушения требований по защите информации в течение года

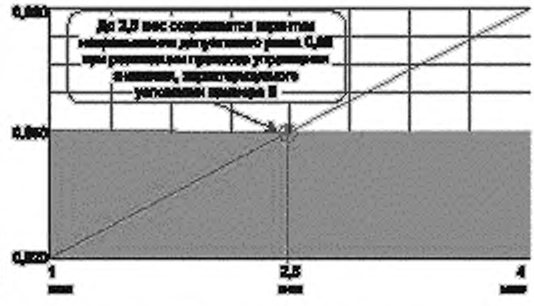


Рисунок Г.7 — Зависимость риска за все центры знаний от периода прогноза длительностью от одного до четырех месяцев

Уровни рисков для угроз выходным результатам ЦЗн1 (связанным с субъективными факторами и ошибками специалистов средней квалификации в области ИТ при решении задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях — элемент 1) и угроз выходным результатам ЦЗн2 (связанным с использованием недекларируемых возможностей программного обеспечения в технологиях дистанционного зондирования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды Арктики — элемент 5) являются определяющими в общем риске нарушения требований по защите информации за год. Причем причиной того, что элемент 1 представляет собой своеобразное «узкое место» в комплексе ЦЗн, является сравнительно высокая частота возникновения источников угроз совершения человеческих ошибок (4 раза в год). А для элемента 5 причиной является сравнительно большое среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы в части выполнения требований по защите информации (через 8 ч) — см. таблицу Г.1.

Г.7.3.2 Пример 6 демонстрирует прогнозирование риска нарушения требований по защите информации с добавлением единого ЦЗн, интегрирующего возможности всех автономных ЦЗн и исполняющего функции резервного центра при различного рода отказах в профильных ЦЗн (вариант 2) — см. рисунок Г.5.

Рассмотрены два случая:

- случай 1: частота возникновение источников угроз возрастает до 1 раза в месяц, что ненамного превышает суммарную частоту возникновения различных источников угроз для ЦЗн1 — ЦЗн5 по таблице Г.1;

- случай 2: частота возникновение источников угроз возрастает до 1 раза в сутки, что в 30 раз превышает частоту по сравнению со случаем 1 и сравнимо с умышленными компьютерными атаками на единый ЦЗн.

Для обоих случаев среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации составляет 1 ч, что свойственно большинству профильных ЦЗн.

Анализ результатов моделирования согласно рекомендациям В.3 для сложной структуры, приведенной на рисунке Г.5, показал следующее.

Для случая 1 в вероятностном выражении суммарный риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,051, т. е. уменьшится по сравнению с примером 5 более чем в 4 раза. Это достигнуто за счет резервирования функционирования профильных центров знаний возможностями единого ЦЗн. При изменении длительности периода прогноза от 6 до 24 мес риск возрастает от 0,015 до 0,161. А для допустимого риска на уровне 0,050 обоснован период до 11,7 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса ЦЗн, характеризуемых условиями случая 1 примера 6 (см. рисунок Г.8).

Для случая 2, ассоциируемого с ежедневными умышленными атаками на единый ЦЗн, суммарный риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,222, т. е. такой же, как для примера 5 с частотой возникновения источников угроз, в 30 раз меньшей. При изменении длительности периода прогноза от 1 до 4 мес риск возрастает от 0,010 до 0,074. А для допустимого риска на уровне 0,050 обоснован период до 2,9 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса центров знаний, характеризуемых условиями случая 2 примера 6 (см. рисунок Г.9).

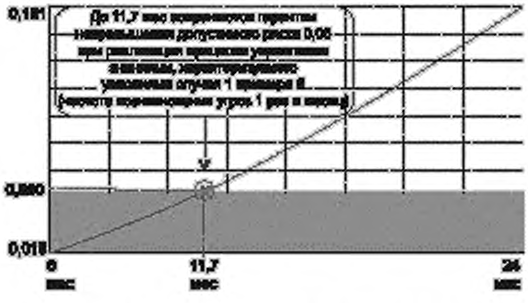


Рисунок Г.8 — Зависимость риска за все ЦЗн от периода прогноза длительностью от 6 до 24 мес (для случая 1)

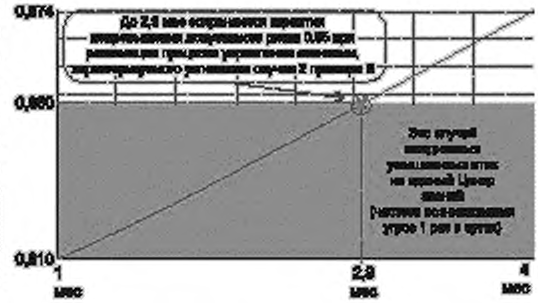


Рисунок Г.9 — Зависимость риска за все ЦЗн от периода прогноза длительностью от 1 до 4 мес (для случая 2 — умышленные атаки)

Г.7.4 Пример 7. В продолжение примеров 1—6 интегральный риск $R_{интегр}(T_{зад})$ нарушения реализации процесса управления знаниями с учетом требований по защите информации рассчитан с использованием рекомендаций раздела В.4.

Учитывая, что период прогноза $T_{зад}$ = 1 год, по результатам расчетов примеров 1—4 имеет место $R_{обобщен}(T_{зад})$ = = 0,030, а по результатам расчетов 6-го примера (случай 2 — умышленные атаки на единый ЦЗн) $R_{наруш}(T_{зад})$ = = 0,051, по формуле (В.10)

$$R_{интегр}(T_{зад}) = 1 - (1 - 0{,}030)\cdot(1 - 0{,}051) \approx 0{,}080.$$

В итоге интегральный риск нарушения реализации процесса управления знаниями о системе в течение года с учетом требований по защите информации составит 0,080. При этом риск нарушения требований по защите информации (0,051) в 1,57 раза меньше обобщенного риска нарушения надежности реализации процесса управления знаниями без учета требований по защите информации. Тем не менее необходим дополнительный поиск мер повышения эффективности защиты информации для непревышения допустимого риска, установленного на уровне 0,050.

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

Примечание — Другие примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59341, ГОСТ Р 59347, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355.

Г.8 Материально-техническое обеспечение

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

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

Г.9 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 управления знаниями о системе

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

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

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

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

Таблица Д.1 — Пример задания допустимых значений рисков

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

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса управления знаниями о системе

Е.1 Методика прогнозирования риска нарушения требований по защите информации в процессе управления знаниями о системе.

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

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

Е.4 Методики выявления явных и скрытых недостатков процесса управления знаниями о системе с использованием прогнозирования рисков.

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

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

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ключевые слова: системная инженерия, защита информации, процесс управления знаниями о системе, актив, безопасность, знания, модель, риск, система, управление

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 29.04.2021. Подписано в печать 17.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5.12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru