ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59341— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ СИСТЕМЫ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 мая 2021 г. № 370-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 5
4 Основные положения системной инженерии по защите информации в процессе управления информацией системы 8
5 Общие требования системной инженерии по защите информации в процессе управления информацией системы 9
6 Специальные требования к количественным показателям 11
7 Требования к системному анализу 13
Приложение А (справочное) Пример перечня защищаемых активов 14
Приложение Б (справочное) Пример перечня угроз 15
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 16
Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса управления информацией системы 34
Приложение Д (справочное) Типовые допустимые значения для расчетных показателей 53
Приложение Е (справочное) Примерный перечень методик системного анализа для процесса управления информацией системы 55
Библиография 56

Введение

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

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

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

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

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

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ СИСТЕМЫ

System engineering. Protection of information in system information management process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа применительно к вопросам защиты информации в процессе управления информацией для систем 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 расчетных показателей 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 информацией системы, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем — см. примеры систем в [1] — [26].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

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

Издание официальное

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

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

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

ГОСТ Р ИСО 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 Шухарта

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

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

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

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 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 27.003, ГОСТ 34.003, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

актив (asset): 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 **актуальность информации:** Свойство безошибочной информации (в том числе подлежащей последующей функциональной обработке или полученной в результате обработки) отражать текущее состояние прикладной области системы со степенью приближения, достаточной для получения на ее основе достоверной выходной информации в интересах конечного пользователя. Актуальность характеризует старение информации во времени.

3.1.3

безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

[ГОСТ Р 50922—2006, статья 2.4.5]

3.1.4 **безошибочность информации:** Свойство информации не иметь явных или скрытых ошибок и/или искажений.

3.1.5

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.6 **достоверность информации:** Свойство информации отражать реальное или оцениваемое состояние объектов и процессов прикладной области со степенью приближения, обеспечивающей эффективное использование этой информации согласно целевому назначению системы. Достоверность выходной информации определяется истинностью исходных данных, безошибочностью входной информации, корректностью обработки, безошибочностью при хранении и передаче информации и сохранением ее актуальности на момент использования.

3.1.7

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]

3.1.8

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

[ГОСТ Р 50922—2006, статья 2.3.4]

3.1.9

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.10

защита информации от несанкционированного доступа; ЗИ от НСД: Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание — Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

[ГОСТ Р 50922—2006, статья 2.3.6]

3.1.11

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

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

3.1.13 **качество используемой информации в системе:** Совокупность свойств используемой информации, обусловливающих ее пригодность для последующего использования в соответствии с целевым назначением в системе.

3.1.14 **качество функционирования системы:** Совокупность свойств, обусловливающих пригодность системы в соответствии с ее целевым назначением.

3.1.15 **корректность обработки информации в системе:** Свойство системы обеспечивать получение правильных согласованных результатов или эффектов обработки информации.

3.1.16 **надежность реализации процесса управления информацией системы:** Свойство процесса управления информацией системы сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить его в заданных условиях реализации с обеспечением качества используемой информации.

3.1.17 **надежность предоставления информации в системе:** Свойство системы обеспечивать прием, автоматическую обработку запроса или команды и предоставление или принудительную выдачу выходной информации согласно функциональному алгоритму при соблюдении эксплуатационных условий применения и технического обслуживания системы.

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

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

3.1.19

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.20

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

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

[ГОСТ Р 57193—2016, пункт 4.1.50]

3.1.21

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.22 **полнота выходной информации в системе:** Свойство выходной информации отражать состояния всех требуемых объектов учета предметной области системы. Слагается из полноты реализации функций системы, полноты ввода первоначальной информации и полноты оперативного отражения объектов учета в системе.

3.1.23 **полнота оперативного отражения объектов учета в системе:** Свойство системы отражать требуемые состояния реально существующих объектов учета, в том числе впервые появляющихся в процессе функционирования системы и подлежащих учету в системе согласно ее функциональному назначению.

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

3.1.25

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, статья 3.2]

3.1.26 **своевременность предоставления требуемой информации в системе:** Свойство системы обеспечивать предоставление запрашиваемой или выдаваемой принудительно (автоматически) выходной информации в задаваемые сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы.

3.1.27 **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.

3.1.28

системная инженерия (systems engineering): 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]

3.1.29 **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.

3.1.30

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

[ГОСТ Р 50922—2006, статья 2.9.2]

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

3.1.32

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.1.33 **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:

БД — база данных;

ГВУ — главная вентиляторная установка;

ЛПР — лицо, принимающее решение;

МДУ — модульная дегазационная установка;

НСД — несанкционированный доступ;

СДК — система дистанционного контроля промышленной безопасности опасного производственного объекта;

ТЗ — техническое задание.

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

4.1 Общие положения

Организации используют процесс управления информацией в рамках создания (модернизации, развития) и эксплуатации системы и взаимодействующих систем, оперирующих с информацией, для обеспечения их безопасности, качества и эффективности, а также при выведении системы из эксплуатации для обоснования принимаемых решений. В процессе управления информацией системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

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

Определение выходных результатов процесса управления информацией системы и типовых действий по защите информации осуществляют по ГОСТ 2.114, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р 51904, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Количественную оценку рисков, свойственных процессу, осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59334, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р МЭК 62508. При этом учитывают специфику создаваемой (модернизируемой) и/или применяемой системы и/или системы, выводимой из эксплуатации, — см., например, [21] — [26].

4.2 Цели процесса и назначение мер защиты информации

4.2.1 Определение целей процесса управления информацией системы осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики рассматриваемой системы.

Настоящий стандарт охватывает техническую, проектную, организационную информацию, информацию соглашений и пользовательскую информацию.

В общем случае целью процесса управления информацией системы является создание, получение, подтверждение, преобразование, сохранение, восстановление, распространение необходимой информации в системе и избавление от ненужной информации. В результате управления обеспечивается надежное и своевременное предоставление заинтересованным сторонам системы полной, достоверной и, если необходимо, конфиденциальной информации для ее использования по назначению.

4.2.2 Меры защиты информации в процессе управления информацией системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59346, ГОСТ Р МЭК 61508-7, [20] — [24] с учетом специфики рассматриваемой системы и реализуемой стадии жизненного цикла.

4.3 Стадии и этапы жизненного цикла системы

Процесс управления информацией системы следует использовать на любой стадии жизненного цикла системы. Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации системы устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом 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 информацией системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

Примечание — К мерам защиты информации относятся также упоминаемые далее в тексте стандарта меры периодической диагностики и восстановления возможностей, меры противодействия угрозам, меры по снижению рисков, корректирующие меры.

4.4 Основные принципы

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

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе управления информацией системы сосредотачивают:

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

5 Общие требования системной инженерии по защите информации в процессе управления информацией системы

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения, а также непосредственно требования по защите информации в процессе управления информацией системы 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 информационные продукцию и/или услуги. Содержание требований по защите информации формируют при выполнении процесса определения системных требований с учетом нормативно-правовых документов Российской Федерации (см., например [1] — [26]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных компонентов — см. ГОСТ Р 59346.

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

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

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

Требования системной инженерии по защите информации в процессе управления информацией системы включают.

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

5.3 Состав выходных результатов и выполняемых действий в процессе управления информацией системы определяют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53647.1, ГОСТ Р 56939, ГОСТ Р 57100, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики рассматриваемой системы.

Примечание — В процессе управления информацией системы необходимо учитывать решение таких вопросов как:

- гарантированное подтверждение достаточности автоматизированной деклассификации конфиденциальной информации (анонимизации, деперсонификации);
- учет возможности повышения уровня конфиденциальности данных в процессе их обработки в системах искусственного интеллекта (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации);
- 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 активы, информация которых или о которых необходима для получения выходных результатов и выполнения действий в процессе управления информацией системы.

Примечание — В состав активов могут быть включены активы, используемые для иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика — например, привлекаемых информационных систем и/или БД поставщиков.

5.5 Определение активов, информация которых или о которых подлежит защите, формирование перечня потенциальных угроз и определение сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ IEC 61508-3, ГОСТ Р 27.403, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57839, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6 и специфики системы (см., например, [21] — [26]).

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

5.6 Эффективность защиты информации при выполнении процесса управления информацией системы анализируют по показателям рисков в зависимости от специфики рассматриваемой 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, представленных в приложениях В, Г, Д, с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1.

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 информацией системы определен в 6.3.

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

6 Специальные требования к количественным показателям

6.1 Общие положения

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

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

- состав информации, подлежащей управлению;
- формы предоставления информации;
- результаты сбора, контроля, обработки, хранения, предоставления информации, подлежащей использованию;
- результаты целенаправленного уничтожения ненужной или недостоверной информации;
- данные о состоянии обеспечения безопасности информации.

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

- определение стратегии управления информацией системы;
- определение информационных объектов, которые подлежат управлению;
- определение полномочий и ответственности при управлении информацией системы;
- определение содержания, форматов и структур информационных объектов;
- определение действий по сопровождению информации (включая анализ статуса хранящейся информации для обеспечения ее полноты, достоверности, безопасности и пригодности);
- сбор, контроль, обработка, хранение и предоставление информации, подлежащей использованию,
- сопровождение информационных объектов и записей об их хранении с регистрацией статуса используемой информации и сохранением возможностей по ее восстановлению,
- обеспечение требуемого уровня безопасности информации для определенных пользователей;
- архивирование информации (при необходимости);
- уничтожение ненужной, недостоверной или недействительной информации.

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 информацией системы с учетом требований по защите информации.

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

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе управления информацией используют следующие количественные показатели:

- риск нарушения надежности реализации процесса управления информацией системы без учета требований по защите информации;
- риск нарушения требований по защите информации в процессе управления информацией системы;
- интегральный риск нарушения реализации процесса управления информацией системы с учетом требований по защите информации.

6.3.2 Риск нарушения надежности реализации процесса управления информацией системы без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса (в зависимости от вероятностей обеспечения надежности и своевременности предоставления информации, полноты и достоверности используемой информации и безошибочности действий пользователей и персонала) в сопоставлении с возможным ущербом.

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

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

6.4 Требования к источникам данных

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

- временные данные функционирования системы защиты информации, в т. ч. данные срабатывания ее исполнительных механизмов;
- текущие и статистические данные о самой системе или о системах-аналогах, характеризующие события о нарушениях надежности и своевременности предоставления информации, полноты и достоверности используемой информации, а также о событиях, связанных с утечкой защищаемой информации, несанкционированными или непреднамеренными воздействиями на защищаемую информацию (привязанные ко временам наступления событий, характеризующих нарушения и предпосылки к нарушениям требований по защите информации);

- текущие и статистические данные результатов технического диагностирования системы защиты информации;

- наличие и готовность персонала системы защиты информации, данные об ошибках персонала (привязанные к временам наступления событий, последовавших из-за этих ошибок и характеризующих нарушения и предпосылки к нарушениям требований по защите информации) в самой системе или в системах-аналогах;

- данные 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 информацией системы включают в себя:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз;
- требования к поддержке принятия решений в жизненном цикле системы.

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 Р 27.403, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, 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 рассматриваемой системы.

Примечание — Примеры решения задач системного анализа применительно к рассматриваемому процессу см. в приложении Г, а применительно к другим процессам — в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе управления информацией системы может включать (в части, свойственной этому процессу):

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

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессе управления информацией системы может включать:

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 56939, ГОСТ Р 58412;

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

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

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

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

- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному заказчику, информация и информационные системы которого были скомпрометированы;

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

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

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе управления информацией системы могут применяться любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Типовые методы и модели обеспечивают вероятностное прогнозирование для следующих показателей:

- риска нарушения надежности реализации процесса управления информацией системы без учета требований по защите информации (см. В.1.2—В.1.7, В.3.1—В.3.7);
- риска нарушения требований по защите информации в процессе управления информацией системы (см. В.2);
- интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3).

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

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

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

В.1.4 Для математической формализации используют следующие основные положения:

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

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

В.1.5 В общем случае критичность задаваемых условий при проведении системного анализа отслеживается с использованием индикаторных функций, которые позволяют учесть различные ограничения, а также формально пренебречь некоторыми менее существенными факторами (формальное влияние которых на уровне вероятностного значения риска не выходит за допустимые количественные пределы с учетом возможного ущерба).

В.1.6 В В.2 представлены модели в контексте нарушения требований по защите информации в приложении к прогнозированию соответствующего риска нарушения требований по защите информации. Изменение контекста позволяет использовать модели для иных приложений (см. способ 1 из В.2.4, В.3 и приложение Г для адаптации математических моделей к контексту нарушения надежности реализации процесса).

В.1.7 В В.2.2 и В.2.3 приведены математические модели для прогнозирования рисков в моделируемой системе, представляемой в виде «черного ящика». Модель В.2.2 для прогнозирования рисков при отсутствии какого-либо контроля является частным случаем модели В.2.3 при реализации технологии периодического системного контроля. Модель В.2.2 применима на практике лишь для оценки и сравнения случая полностью бесконтрольного функционирования моделируемой системы, например, там, где контроль невозможен или нецелесообразен по функциональным, экономическим или временным соображениям, или когда ответственные лица пренебрегают

функциями контроля или не реагируют должным образом на результаты системного анализа. Для моделируемых систем сложной структуры применимы методы, изложенные в В.2.4, включая методы комбинации и повышения адекватности моделей.

В.1.8 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы. Для исследования запроектных сценариев при моделировании могут быть использованы гипотетичные исходные данные.

Примечание — Другие возможные подходы для оценки вероятностных показателей и подходы, подобные изложенным в В.2 — В.4, описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

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

В.2.1 Пространство элементарных событий

В приложении к контексту защиты информации в моделях простой структуры под моделируемой системой понимается определенный выходной результат или совокупность задействованных активов, рассматриваемых как единое целое, или отдельное действие или совокупность действий, рассматриваемых как единое целое, к которым предъявлены требования и применяются идентичные меры защиты информации. Такую систему рассматривают как «черный ящик», для него сделано предположение об использовании одной и той же модели угроз и одной и той же технологии системного контроля выполнения требований по защите информации и восстановлению 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 «черный ящик». В общем случае для системы сложной структуры для различных элементов могут быть применены различные модели угроз или различные технологии системного контроля выполнения требований по защите информации и восстановлению системы.

При моделировании, направленном на прогнозирование риска нарушения требований по защите информации, целевое назначение моделируемой системы проявляется в выполнении требований по защите информации. Такая интерпретация подразумевает выполнение требований по защите информации не только применительно к защищаемым активам и действиям, с использованием которых создают и получают выходные результаты, но и к самим выходным результатам, которые применяют (или планируют к созданию, получению и/или применению). В итоге для каждого из элементов моделируемой системы и системы в целом в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных событий на временной оси образуют два основных состояния:

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

В результате математического моделирования рассчитывают вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение до 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.2.2 Математическая модель «черного ящика» при отсутствии какого-либо контроля

Моделируемая система представлена в виде «черного ящика», функционирование которого не контролируется. Восстановление возможностей по выполнению требований по защите информации осуществляется по мере нарушения. При функционировании в результате возникновения угроз и их развития может произойти нарушение возможностей по выполнению требований по защите информации. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения требований по защите информации в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения требований по защите информации в процессе управления информацией системы в течение заданного периода прогноза при отсутствии какого-либо контроля.

Модель представляет собой частный случай модели В.2.3, если период между диагностиками выполнения требований по защите информации больше периода прогноза. Учитывая это, используют формулы (В.1) — (В.5) из В.2.3.

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

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

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

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

Развитие событий в моделируемой системе считается не нарушающим требований по защите информации в течение заданного периода прогноза, если к началу этого периода выполнение требований по защите информации обеспечено и в течение всего периода либо источники угроз не активизируются, либо после активизации до реализации угроз происходит их своевременное выявление и принятие адекватных мер противодействия угрозам. В целях моделирования предполагают, что существуют не только средства контроля (диагностики) выполнения требований по защите информации, но и способы поддержания и/или восстановления возможностей по обеспечению их выполнения при выявлении источников или следов начала активизации угроз. Восстановление осуществляется лишь в период системного контроля (диагностики). Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии ненарушения требований по защите информации из-за возможных угроз в период прогноза (т. к. в принятой модели за счет предупреждающих действий по результатам диагностики устраняются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент нанесения ущерба от реализации какой-либо угрозы).

За основу анализа принят следующий последовательный алгоритм возникновения и развития потенциальной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться, представляя возможную угрозу для нарушения требований по защите информации. По прошествии периода активизации, свойственного этому источнику угрозы (в общем случае этот период активизации представляет собой случайную величину), наступает виртуальный момент непосредственно реализации угрозы, интерпретируемый как момент нарушения требований по защите информации с возможными негативными последствиями. Если после виртуального начала активизации угрозы на временной оси наступает очередная диагностика целостности моделируемой системы, то дальнейшая активизация угрозы полагается предотвращенной до нанесения недопустимого ущерба, а источник угроз — нейтрализованным (до возможного нового появления какой-либо угрозы после прошедшей диагностики).

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

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

С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения требований по защите информации в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели является расчетная вероятность нарушения требований по защите информации в процессе управления информацией системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики). При этом учитываются предпринимаемые меры периодической диагностики и восстановления возможностей по выполнению требований по защите информации.

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

σ — частота возникновения источников угроз в моделируемой системе с точки зрения нарушения требований по защите информации в процессе управления информацией системы;

β — среднее время развития угроз с момента возникновения источников угроз 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 выполнению требований по защите информации в системе;

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

$T_{восст}$ — среднее время восстановления нарушенных возможностей по выполнению требований по защите информации в системе (учитывают путем использования способа 4 из В.2.4);

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

Примечание — Переопределения этих исходных данных, конкретизированные в приложении к выходным результатам и действиям процесса согласно способу 1 из В.2.4, приведены в Г.7.

В общем случае оценку вероятности нарушения требований по защите информации в моделируемой системе $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ осуществляют по формуле:

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

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

В настоящем подразделе определены расчетные выражения для случая, когда значения средних времен системной диагностики $T_{\text{диаг}}$ и восстановления нарушенных возможностей по выполнению требований по защите информации $T_{\text{восст}}$ равны, т. е. для этого случая $P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}}) = P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$. Расчет для более общего случая, когда значения $T_{\text{диаг}}$ и $T_{\text{восст}}$ различны, осуществляется с использованием 4-го способа повышения адекватности моделей (см. В.2.4).

Возможны два варианта:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

В итоге вероятность отсутствия нарушений требований по защите информации в течение периода прогноза $T_{\text{зад}}$ определяется аналитическими выражениями (В.2) — (В.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (В.1) вероятность нарушения требований по защите информации в системе $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ в течение заданного периода прогноза $T_{\text{зад}}$ с учетом

предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по выполнению требований по защите информации в системе. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения требований по защите информации в процессе управления информацией системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

Примечание — В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель В.2.3 превращается в модель В.2.2 для прогноза риска нарушения требований по защите информации в моделируемой системе при отсутствии какого-либо контроля.

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

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

Расчет основан на применении следующих инженерных способов.

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

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



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

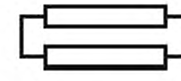


Рисунок В.2 — Система из параллельно соединенных элементов («ИЛИ»)

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

- для моделируемой системы из двух последовательно соединенных элементов

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

- для моделируемой системы из двух параллельно соединенных элементов

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

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

Примечание — Если для достижения своих целей нарушитель вынужден преодолевать несколько преград, защита моделируется с использованием параллельно соединяемых элементов. С точки зрения защиты логическое соединение «ИЛИ» для двух преград интерпретируется так (см. рисунок В.3): система защиты из двух преград сохраняет свои возможности по выполнению требований по защите информации в течение времени t, если 1-я преграда «ИЛИ» 2-я преграда сохраняют свои возможности по выполнению требований по защите информации в течение этого времени, не позволяя нарушителю достичь своей цели путем преодоления всех преград.

Рекурсивное применение соотношений (В.6), (В.7) «снизу-вверх» обеспечивает получение соответствующих вероятностных оценок для сколь угодно сложной логической структуры с параллельно-последовательным логическим соединением элементов.

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

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

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

- 1-я итерация определяет $T^{(1)}_{диаг} = T_{диаг}$, задаваемое на входе модели. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемых возможностей по выполнению процесса (т. е. в рамках времени диагностики);

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

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

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

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

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

где $R^{(r-1)}$ вычисляют по моделям В.2.2, В.2.3, но в качестве исходного уже выступает $T^{(r-1)}_{диаг}$, рассчитанное на предыдущем шаге итерации. Здесь в большей степени учитывается время восстановления с частотой, стремящейся к реальной. Соответственно риск $R^{(r-1)}$ также приближается к реальному.

С увеличением r указанная последовательность $T^{(r)}_{диаг}$ сходится, и для дальнейших расчетов используют значение, отличающееся от точного предела $T^{(\infty)}_{диаг}$ на величину, пренебрежимо малую по сравнению с задаваемой изначально точностью ε расчетов при итерации:

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

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

$T_{диаг}$ — среднее время системной диагностики возможностей по выполнению требований по защите информации в моделируемой системе;

$T_{восст}$ — среднее время восстановления нарушенных возможностей по выполнению требований по защите информации в моделируемой системе.

При этом для расчетов применяются одни и те же модели В.2.2 и В.2.3. В результате обеспечена возможность расчета показателей $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ и $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ по формулам (В.1) — (В.7).

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

Применение инженерных способов 1—4 обеспечивает более точный прогноз вероятности нарушения требований по защите информации для системы сложной структуры с учетом различий во временах диагностики и восстановления целостности моделируемой системы. Этой расчетной вероятности нарушения требований по защите информации в системе при оценке рисков сопоставляют возможный ущерб.

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

В.3.1 Общие положения

В.3.1.1 Модели В.3 позволяют оценить свойство процесса управления информацией системы сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях реализации с обеспечением надежности и своевременности предоставления, полноты, достоверности и безопасности используемой информации. Достоверность выходной информации определяется истинностью исходных данных, безошибочностью входной информации, корректностью обработки, безошибочностью при хранении и передаче информации и сохранением ее актуальности на момент использования. Осуществляют учет «человеческого фактора» на уровне безошибочности действий пользователей и персонала системы. В свою очередь безопасность информации характеризуется таким состоянием ее защищенности, при котором обеспечены конфиденциальность, доступность и целостность информации.

Оценки осуществляют с использованием вероятностных показателей нахождения моделируемой системы в определенном элементарном состоянии. В сопоставлении с возможным ущербом эти вероятностные оценки характеризуют соответствующие риски. Для прогнозирования рисков нарушения надежности реализации процесса управления информацией в моделируемой системе без учета требований по защите информации востребованы и подлежат использованию модели (см. В.3.2 — В.3.8), предназначенные для оценки:

- надежности предоставления используемой информации;
- своевременности предоставления используемой информации;
- полноты оперативного отражения в системе новых объектов и явлений;
- актуальности обновляемой информации;
- безошибочности информации после контроля;
- корректности обработки информации;
- оценки безошибочности действий пользователей и персонала системы.

Примечание — Определение ошибки и влияние человеческого фактора на надежность — по ГОСТ Р МЭК 62508.

В.3.1.2 С учетом необходимости детализации модели угроз безопасности информации на практике может быть востребована аналитическая адаптация моделей В.2 с тем, чтобы обеспечить детализацию в прогнозировании риска нарушения требований по защите информации (см. В.3.9). К таким адаптируемым моделям относятся математические модели для оценки:

- сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий;
- защищенности активов от несанкционированного доступа;
- сохранения конфиденциальности используемой информации.

В.3.1.3 Прогнозирование интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации должно учитывать результаты моделирования по моделям В.2 с учетом положений В.3.1.1, В.3.1.2.

В.3.1.4 В терминах моделируемой системы, отождествляемой с выполняемыми действиями, под целостностью моделируемой системы понимается такое состояние характеристик реализуемых действий, которое в течение задаваемого периода прогноза отвечает требованиям обеспечения надежности и своевременности предоставления запрашиваемой или выдаваемой принудительно информации, полноты, достоверности и безопасности используемой информации. С точки зрения системного анализа пространство элементарных событий отдельного действия (как элемента моделируемой системы) на временной оси образуют следующие основные состояния:

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

- «Целостность элемента моделируемой системы нарушена» — в противном случае.

При этом под целостностью элемента моделируемой системы понимается такое состояние этого элемента, которое в течение задаваемого периода прогноза отвечает целевому назначению системы. С учетом логических условий «И» и «ИЛИ» устанавливают элементарные состояния для каждого элемента и моделируемой системы в целом.

В.3.2 Модели для оценки надежности предоставления информации

Модели позволяют оценить вероятность надежного предоставления запрашиваемой или выдаваемой принудительно информации в системе в течение заданного периода прогноза $P_{\text{над предст}}(T_{\text{зад}})$.

В моделях для оценки надежности предоставления информации под системой понимается отдельное действие или множество действий процесса управления информацией системы, выполняемых с использованием определенных защищаемых активов. Для каждого из анализируемых действий возможно либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения этого действия. Модели представлены в В.3.2.1, В.3.2.2.

В.3.2.1 Математическая модель для оценки надежности при отсутствии какого-либо контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением формализации по модели В.2.2. Специфика состоит в логическом переопределении исходных данных для моделирования (см. также приложение Г). Это означает применение способа 1 из В.2.4. Формально модель позволяет оценить вероятностное значение риска нарушения целостности моделируемой системы в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели с учетом возможного ущерба является расчетный риск нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в системе в течение заданного периода прогноза при отсутствии какого-либо контроля. Применимы методы повышения адекватности из В.2.4.

Модель применяют для случая, когда в системе отсутствует какой-либо контроль (диагностика) целостности реализуемых действий процесса. Модель представляет собой частный случай моделей В.2.3 и В.3.2.2, если период между диагностиками целостности моделируемой системы больше периода прогноза.

В.3.2.2 Математическая модель для оценки надежности при реализации технологии периодического системного контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением математической формализации по модели В.2.3. Специфика состоит в логическом переопределении исходных данных для моделирования (см. также приложение Г). С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели с учетом возможного ущерба является расчетный риск нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в системе в течение заданного периода прогноза при реализации технологии периодического системного контроля. Применимы методы повышения адекватности по В.2.4.

Для расчета риска нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в моделируемой системе исходные данные формально переопределяют применительно к выполняемым действиям и защищаемым активам:

σ — частота возникновения источников угроз с точки зрения нарушения надежности предоставления информации;

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

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

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

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

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

Примечание — Несмотря на фактическую повторяемость некоторых названий исходных данных, их значения при моделировании с использованием модели В.3.2 будут отличны от значений при использовании модели В.2.3, поскольку различны их природа, причины формирования значений, интерпретация и области приложений. Соответственно разными будут и расчетные риски.

В итоге расчетная вероятность надежного предоставления информации характеризуется вероятностью отсутствия нарушений целостности моделируемой системы в течение периода прогноза $T_{\text{зад}}$ и определяется теми же аналитическими выражениями (В.1) — (В.9), что и в моделях В.2.2, В.2.3, В.2.4, в зависимости от варианта соотношений между исходными данными.

Сопоставление с возможным ущербом позволяет рассматривать расчетную вероятность по формуле (В.1) как риск нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в системе в течение заданного периода прогноза с учетом предпринимаемых технологических мер периодического

системного контроля и восстановления целостности моделируемой системы. Вероятностное значение этого риска представляет собой дополнение до единицы вероятности надежного предоставления запрашиваемой или выдаваемой принудительно информации в течение заданного периода прогноза.

В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель В.3.2.2 превращается в модель В.3.2.1 для прогноза риска при отсутствии какого-либо контроля.

Таким образом, модели В.3.2 позволяют оценивать надежность предоставления запрашиваемой или выдаваемой принудительно информации, подлежащей использованию в системе.

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ над}(T_{зад})$ и условие α. Условие α касается надежности предоставления запрашиваемой или выдаваемой принудительно информации и формулируется в виде ограничений: $P_{над\ предст}(T_{зад}) \geq P_{доп\ над}(T_{зад})$ и возможный ущерб от нарушения не превышает допустимого (это — формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента надежности предоставления информации $Z_{над\ предст}(T_{зад})$

$$Z_{над\ предст}(T_{зад}) = \begin{cases} 1, \text{ если условие надежности предоставления информации } \alpha \text{ выполнено,} \\ P_{над\ предст}(T_{зад}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.10)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $[1 - Z_{над\ предст}(T_{зад})]$ в качестве вероятностного выражения риска нарушения надежности предоставления запрашиваемой или выдаваемой принудительно информации в системе.

Выполнение требований по своевременности предоставления информации, полноты, достоверности и безопасности используемой информации с соблюдением требований по защите информации учтено в В.3.3 — В.3.9.

В.3.3 Модель для оценки своевременности предоставления информации

Модель позволяет оценить вероятностно-временные показатели обработки в системе информации различных типов и интегрирующие показатели: относительную долю своевременно обработанных запросов $C_{своевр}$ и коэффициент своевременности обработки запросов $Z_{своевр}$.

Для каждого из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) требования к своевременности обработки запросов в системе (касающиеся как запрашиваемой, так и выдаваемой принудительно информации) формулируют с применением одного из двух критериев:

- критерия своевременности по среднему времени реакции: среднее время обработки запросов i-го типа T_i должно быть не более задаваемого $T_{зад\ i}$ (далее условие этого критерия упоминается как условие своевременности α_1);

- вероятностного критерия: вероятность своевременной обработки запросов i-го типа в системе $P_{св\ i}(T_{зад\ i}) = P_{св\ i}(\tau_i \leq T_{зад\ i})$ за заданное время $T_{зад\ i}$ должна быть не ниже задаваемой $P_{св\ зад\ i}$ (далее условие этого критерия упоминается как условие своевременности α_2), где τ_i — случайная величина, означающая время реакции системы при обработке запросов i-го типа.

Среднее время реакции моделируемой системы и среднеквадратичное отклонение времени реакции при обработке запросов определяют с использованием натурных экспериментов или с использованием моделей теории массового обслуживания. Вероятность своевременной обработки запросов определяют с использованием табулируемой неполной гамма-функции:

$$P_{св\ i}(T_{зад\ i}) = \int_0^{\theta_i} \exp(-\tau)\tau^{\gamma_i} d\tau / \Gamma(\gamma_i), \quad (В.11)$$

где $\Gamma(\gamma) = \int_0^{\infty} \exp(-\tau)\tau^{\gamma} d\tau$ — гамма-функция, $\gamma_i = \dfrac{T_i}{\sqrt{T_{i2} - T_i^2}}$, $\theta_i = T_{зад\ i} \cdot \dfrac{\gamma_i^2}{T_i}$;

γ_i, θ_i — рассчитываемые параметры неполной гамма-функции;

T_i и $(T_i^2 - T_{i2})^{0,5}$ — соответственно среднее время и среднеквадратичное отклонение времени реакции системы при обработке запросов i-го типа (т. е. полного времени пребывания на обработке с учетом ожидания в очередях), T_{i2} — второй момент времени реакции. Чаще в качестве исходных данных формируют целиком именно среднеквадратичное отклонение, не опускаясь до отдельных измерений второго момента.

Примечание — Для инженерных расчетов вероятности своевременной обработки запросов учитывают, что экспоненциальная аппроксимация распределения времени реакции позволяет получать пессимистические оценки (т. е. оценки сверху), при этом среднее время реакции и среднеквадратичное отклонение времени реакции совпадают.

Для оценок эффективности по всему множеству запросов различных типов, сравнения различных вариантов последовательности обработки запросов и настройки параметров используют следующие показатели относительной доли своевременно обработанных в системе запросов и коэффициентом своевременности обработки запросов.

Относительная доля своевременно обработанных в системе запросов $C_{своевр}$ охватывает лишь те типы запросов, для которых выполнены требования заказчика, этот показатель вычисляют по формуле

$$C_{своевр} = \sum_{i=1}^{J} \lambda_i P_{св\ i}(T_{зад\ i}) \left[Ind(\alpha_1) + Ind(\alpha_2) \right] / \sum_{i=1}^{J} \lambda_i, \quad (В.12)$$

где λ_i — частота поступления на обработку запросов i-го типа.

Критерии своевременности обработки каждого типа запросов устанавливают с использованием индикаторной функции $Ind\ (\alpha)$:

$$Ind(\alpha) = \begin{cases} 1, & \text{если условие } \alpha \text{ истинно,} \\ 0, & \text{если условие } \alpha \text{ ложно.} \end{cases}$$

При этом для i-го типа запросов условие своевременности α с учетом возможных ущербов определяют одним из условий α_1 или α_2:

- α_1 — условие, когда для i-го типа запросов задан критерий своевременности по среднему времени реакции и $T_i \le T_{зад\ i}$;

- α_2 — условие, когда для i-го типа запросов задан вероятностный критерий своевременности и $P_{св\ i}(\tau_i \le T_{зад\ i}) \ge P_{св\ зад\ i}$.

Для оценки интегрального риска условие своевременности предоставления информации α формулируют в виде условий α_1 или α_2 с добавлением, что в случае их нарушения возможный ущерб не превышает допустимого (это — формулировка условия α по всем типам запросов). Учет результатов моделирования осуществляют с использованием индикаторного коэффициента своевременности обработки запросов $Z_{своевр}$

$$Z_{своевр} = \begin{cases} 1, & \text{если условия своевременности } \alpha \text{ выполнены для всех типов запросов,} \\ C_{своевр} & \text{по (В.12), если хотя бы одно условие не выполнено.} \end{cases} \quad (В.13)$$

Необходимые для моделирования границы исходных значений λ_i, $T_{зад\ i}$, $P_{св\ зад\ i}$ задают в ТЗ или в постановках функциональных задач для рассматриваемой системы, а значения среднего времени и среднеквадратичного отклонения времени реакции моделируемой системы при обработке запросов i-го типа устанавливают в результате натурных испытаний, экспериментов, дополнительного моделирования или сравнения с аналогами.

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{своевр})$ в качестве вероятностного выражения риска нарушения своевременности предоставления запрашиваемой или выдаваемой принудительно информации в системе.

В.3.4 Модель для оценки полноты оперативного отражения в системе новых объектов и явлений

Модель позволяет оценить вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{полн}$.

До момента, пока новые объекты и явления, ранее не учтенные и появившиеся в динамике функционирования системы, не охвачены ею, для пользователей формально отсутствует полнота оперативного отражения требуемых объектов учета. Требуемая полнота обеспечивается на основе реализации в системе рациональных технологий выявления и сбора первоначальных данных, подлежащих в последующем обновлению.

В предположении пуассоновского потока новых объектов и явлений вероятность обеспечения полноты оперативного отражения в БД системы $P_{полн}$ новых реально существующих объектов и явлений вычисляют по формуле

$$P_{полн} = \exp(-\lambda \cdot T_{база\ данных}), \quad (В.14)$$

где λ — частота появления новых объектов и явлений в процессе функционирования системы;

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода новых объектов учета в БД системы.

Необходимые для моделирования границы исходных значений λ задают в постановках функциональных задач, а значения $T_{база\ данных}$ устанавливают в результате натурных испытаний, экспериментов, дополнительного моделирования или сравнения с аналогами.

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ полн}$ и условие α. Условие α касается полноты оперативного отражения в системе новых объектов и явлений и формулируется в виде ограничений: $P_{полн} \ge P_{доп\ полн}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием вероятностного коэффициента полноты оперативного отражения в системе новых объектов и явлений $Z_{полн}$

$$Z_{полн} = \begin{cases} 1, & \text{если условие полноты отражения в системе объектов и явлений } \alpha \text{ выполнено,} \\ P_{полн}, & \text{если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.15)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{полн})$ в качестве вероятностного выражения риска нарушения полноты оперативного отражения в системе новых объектов и явлений.

В.3.5 Модель для оценки актуальности обновляемой информации

Модель позволяет оценить вероятность сохранения актуальности информации в системе на момент ее использования $P_{акт}$.

После первоначального отражения в системе данных о реально существующих объектах и явлениях эти данные естественным образом устаревают со временем, т. е. теряют свою актуальность для выполнения системой своих функций. Требуемая актуальность обновляемых данных обеспечивается на основе своевременного выявления значимых изменений, реализации эффективных технологий обновления данных в системе, а также за счет достаточно частого обновления применяемых данных в БД.

При экспоненциальной аппроксимации распределений исходных характеристик и их независимости вероятность сохранения актуальности информации в системе $P_{акт}$ на момент ее использования вычисляют по формулам:

- для дисциплины выдачи данных от источника сразу по происшествии значимого изменения состояния объектов учета и явлений

$$P_{акт} = \frac{\xi}{\xi + T_{база\ данных}}; \quad (В.16)$$

- для дисциплины обновления информации в системе вне зависимости от наличия или отсутствия изменения текущего состояния объектов учета и явлений

$$P_{акт} = \frac{\xi^2}{(\xi + T_{база\ данных})(\xi + q)}. \quad (В.17)$$

В случае, когда обновление информации в системе осуществляется строго через постоянный интервал времени q, используют формулу

$$P_{акт} = \frac{\xi^2}{q(\xi + T_{база\ данных})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right], \quad (В.18)$$

где ξ — среднее время между значимыми изменениями реальной информации относительно информации, хранимой в системе (т. е. ξ^{-1} — частота значимого изменения);

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода в БД данных от источников информации;

q — среднее время между соседними обновлениями данных (т. е. q^{-1} — частота обновления данных) в системе.

Необходимые для моделирования границы исходных значений ξ задают в постановках функциональных задач, значения $T_{база\ данных}$ устанавливают в результате натурных испытаний, экспериментов, дополнительного моделирования или сравнения с аналогами, дисциплину обновления данных в системе и значения q указывают в эксплуатационной документации (в части регламента обновления данных).

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ акт}$ и условие α. Условие α касается сохранения актуальности информации в системе на момент ее использования и формулируется в виде ограничений: $P_{акт} \geq P_{доп\ акт}$ и возможный ущерб от нарушения не превышает допустимого (это — формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента актуальности информации в системе $Z_{акт}$

$$Z_{акт} = \begin{cases} 1, & \text{если условие сохранения актуальности информации в системе } \alpha \text{ выполнено,} \\ P_{акт}, & \text{если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.19)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{акт})$ в качестве вероятностного выражения риска нарушения актуальности информации в системе на момент ее использования.

В.3.6 Модель для оценки безошибочности информации после контроля

Модель позволяет оценить вероятность отсутствия ошибок в информации после ее контроля $P_{безош}$, а также вероятность отсутствия ошибок в информации без ее контроля и ожидаемую долю ошибок после контроля.

Информация считается безошибочной в результате контроля, если в процессе контроля до истечения заданного срока контроля все наличествующие ошибки выявлены (и, соответственно, исправлены) и новые ошибки не внесены. Требуемая безошибочность информации в системе после контроля обеспечивается на основе использования эффективных средств и способов выявления и исправления ошибок и рациональной регламентации работы контролера (в качестве контролера могут выступать программно-технические средства системы, человек-контролер или их комбинация).

Для описания процессов контроля безошибочности информации приняты следующие обозначения:

V — объем контролируемой информации;

μ — доля первоначальных ошибок в контролируемой информации в объеме V (до контроля), т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν — средняя скорость контроля информации;

n — частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки);

$T_{нар}$ — среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной (для программно-технических средств — это время наработки на отказ);

$T_{непр}$ — период непрерывной работы контролера;

$T_{зад}$ — задаваемое время на контроль информации.

Возможны 4 варианта соотношений между временем реального контроля $T_{реальн}$ всего объема документа ($T_{реальн} = V/\nu$), задаваемым допустимым временем контроля $T_{зад}$ и непрерывным временем работы контролера $T_{непр}$.

Вариант 1. Задаваемое допустимое время контроля не меньше, чем время реального контроля (т. е. $T_{реальн} \le T_{зад}$), а объем контролируемой информации относительно мал, что позволяет проверить его за один период непрерывной работы контролера ($T_{реальн} \le T_{непр}$).

Для экспоненциальной аппроксимации распределений интервалов между ошибками в контролируемой информации, времени до свершения ошибки 1-го рода и времени наработки контролера на ошибку, а также при условии независимости исходных характеристик вероятность $P_{после(1)}(V, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$ отсутствия ошибок в информации после контроля для варианта 1 вычисляют по формуле

$$P_{после(1)} = \begin{cases} e^{-nV/\nu}\left[T_{нар}^{-1}e^{-\mu V} - \mu\nu e^{-V/(\nu T_{нар})}\right] / \left(T_{нар}^{-1} - \mu\nu\right), \text{ если } T_{нар}^{-1} \ne \mu\nu, \\ e^{-(n+\mu\nu)V/\nu}\left[1 - V\mu\right], \text{ если } T_{нар}^{-1} = \mu\nu. \end{cases} \quad (B.20)$$

Вариант 2. Задаваемое допустимое время контроля не меньше, чем время реального контроля (т. е. $T_{реальн} \le T_{зад}$), но объем контролируемой информации относительно большой ($T_{реальн} > T_{непр}$). Это требует нескольких (N) периодов непрерывной работы контролера, в общем случае $N = V/(\nu T_{непр})$. Внутри каждого периода проверяют часть всего объема, равную в среднем $V_{части(2)} = V/N$ а допустимое время контроля информации для этой части принимают равным $T_{зад\ части\ (2)} = T_{зад}/N$. Тем самым для каждой контролируемой части выполняются условия варианта 1. Вероятность $P_{после(2)} = P_{после(2)}(V, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$ отсутствия ошибок в информации всего объема после контроля для варианта 2 вычисляют по формуле

$$P_{после(2)} = \{P_{после(1)}(V_{части(2)}, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад\ части\ (2)})\}^N. \quad (B.21)$$

Вариант 3. Задаваемое допустимое время контроля меньше, чем время реального контроля ($T_{реальн} > T_{зад}$) при задаваемой средней скорости контроля ν, т. е. объективно может быть проверена лишь часть от всего объема информации, равная $V_{части(3)} = \nu T_{зад}$. В свою очередь, сам объем контролируемой информации относительно мал и может быть проверен за один период непрерывной работы контролера, т. е. $T_{реальн} \le T_{непр}$ и для проверяемого объема $V_{части(3)}$ выполняются условия варианта 1. Вероятность $P_{после(3)} = P_{после(3)}(V, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$ отсутствия ошибок в информации всего объема после контроля для варианта 3 вычисляют по формуле

$$P_{после(3)} = [V_{части(3)}/V] \cdot P_{после(1)}(V_{части(3)}, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад}) + [(V - V_{части(3)})/V] \cdot P_{без\ контроля}, \quad (B.22)$$

где вероятность отсутствия ошибок в непроверенной части информации $V - V_{части(3)}$ равна $P_{без\ контроля} = e^{-\mu(V - V_{части(3)})}$, а вероятность отсутствия ошибок в объеме проверенной информации равна $P_{после(1)}(V_{части(3)}, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$.

Вариант 4. Задаваемое допустимое время контроля меньше, чем время реального контроля ($T_{реальн} > T_{зад}$), но объем контролируемой информации относительно большой ($T_{реальн} > T_{непр}$). Аналогично варианту 3 реально может быть проверена лишь часть от всего объема, равная $V_{части(4)} = \nu T_{зад}$. Относительно этой части возможны два подварианта:

- подвариант 4.1: $T_{зад} \le T_{непр}$, т. е. проверка будет завершена за один период непрерывной работы контролера;
- подвариант 4.2: $T_{зад} > T_{непр}$, т. е. потребуется несколько (N) периодов непрерывной работы контролера $N = V_{части(4)}/(\nu T_{непр})$.

Для подварианта 4.1 вероятность $P_{после(4.1)} = P_{после(4.1)}(V, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$ отсутствия ошибок в информации после контроля вычисляют по формуле

$$P_{после(4.1)} = [V_{части(4)}/V] \cdot P_{после(1)}(V_{части(4)}, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад}) + [(V - V_{части(4)})/V] \cdot e^{-\mu(V - V_{части(4)})}. \quad (B.23)$$

Для подварианта 4.2 внутри каждого периода проверяют новую часть, равную в среднем $V_{части(4.2)} = V_{части(4)}/N$, и допустимое время контроля для этой новой части принимают равным $T_{зад\ части\ (4.2)} = T_{зад}/N$.

Вероятность $P_{после(4.2)} = P_{после(4.2)}(V, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад})$ отсутствия ошибок в информации после контроля вычисляют по формуле

$$P_{после(4.2)} = [V_{части(4)}/V] \cdot \{P_{после(1)}(V_{части(4.2)}, \mu, \nu, n, T_{нар}, T_{непр}, T_{зад\ части\ (4.2)})\}^N + [(V - V_{части(4)})/V] \cdot e^{-\mu(V - V_{части(4)})}. \quad (B.24)$$

В итоге вероятность отсутствия ошибок в информации после ее контроля $P_{безош} = P_{после}$ определяется аналитическими выражениями для $P_{после\ (1)}$, $P_{после\ (2)}$, $P_{после\ (3)}$, $P_{после\ (4.1)}$, $P_{после\ (4.2)}$, в зависимости от варианта соотношений между исходными данными.

Для всех четырех вариантов доля ошибок после контроля $\mu_{после} = \mu \cdot (1 - P_{после})$.

Понятие ошибки должно быть определено. Необходимые для моделирования границы исходных значений V, $T_{зад}$ задают в ТЗ или постановках функциональных задач, диапазон возможных значений μ, ν, n, $T_{нар}$ устанавливают в результате натурных экспериментов или дополнительного моделирования, значение $T_{непр}$ указывают в эксплуатационной документации (в части регламента работы контролера). При отсутствии данных в документации системы используют статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные.

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ безош}$ и условие α. Условие α касается обеспечения безошибочности информации после контроля и формулируется в виде ограничений: $P_{безош} \geq P_{доп\ безош}$ и возможный ущерб от нарушения не превышает допустимого (это — формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочности информации в системе $Z_{безош}$

$$Z_{безош} = \begin{cases} 1, \text{ если условие безошибочности информации после контроля } \alpha \text{ выполнено,} \\ P_{безош}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.25)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{безош})$ в качестве вероятностного выражения риска нарушения безошибочности информации в системе после ее контроля.

В.3.7 Модель для оценки корректности обработки информации

Модель позволяет оценить вероятность получения корректных результатов обработки информации $P_{корр}$.

Информация считается корректно обработанной, если в процессе ее анализа до истечения заданного срока обработки все принципиальные моменты учтены и алгоритмические ошибки не допущены. Требуемая корректность обработки информации программно-аналитическими средствами в системе и выходной информации от системы пользователями обеспечивается на основе применения эффективных способов анализа информации (как с использованием, так и без использования прикладного программного обеспечения), позволяющих учесть важную для принятия решения информацию и не допустить алгоритмических ошибок при анализе всего объема информации. Корректность в обработке информации является следствием приемлемого соотношения между объемом анализируемой информации, частью важной для принятия решения информации, подлежащей учету, скоростью анализа информации, частотой ошибок аналитика, длительностью его непрерывной работы и ограничениями на допустимое время обработки.

Формализация процессов обработки информации в системе полностью аналогична формализации для модели В.3.6 с точностью до переопределений исходных данных (см. способ 1 из В.2.4):

V — объем информации, подлежащий обработке (анализу);

μ — часть важной для принятия решения информации, которая должна быть объективно использована при обработке (анализе) информации объема V, т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν — скорость обработки (анализа);

n — частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной);

$T_{нар}$ — среднее время наработки на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это — аналог ошибки контроля 2-го рода);

$T_{непр}$ — период непрерывной работы аналитика (в качестве аналитика могут выступать программно-аналитические средства или пользователь системы);

$T_{зад}$ — задаваемое время на обработку (анализ) информации. Вероятность $P_{корр}$ (V, μ, ν, n, $T_{нар}$, $T_{непр}$, $T_{зад}$) получения корректных результатов обработки (анализа) информации равна

$$P_{корр} = \begin{cases} P_{после(1)} \text{ при } V / \nu \leq T_{зад} \text{ и } V / \nu \leq T_{непр}; \\ P_{после(2)} \text{ при } V / \nu \leq T_{зад} \text{ и } V / \nu > T_{непр}; \\ P_{после(3)} \text{ при } V / \nu > T_{зад} \text{ и } V / \nu \leq T_{непр}; \\ P_{после(4.1)} \text{ при } V / \nu > T_{зад},\ V / \nu > T_{непр} \text{ и } T_{зад} \leq T_{непр}; \\ P_{после(4.2)} \text{ при } V / \nu > T_{зад},\ V / \nu > T_{непр} \text{ и } T_{зад} > T_{непр}, \end{cases}$$

где $P_{после(1)}$, $P_{после(2)}$, $P_{после(3)}$, $P_{после(4.1)}$, $P_{после(4.2)}$ вычисляют по формулам (В.20) — (В.24).

Необходимые для моделирования границы исходных значений V, $T_{зад}$ задают в ТЗ или в постановках функциональных задач, диапазон возможных значений μ, ν, n, $T_{нар}$ устанавливают в результате натурных эксперимен-

тов или дополнительного моделирования, значение $T_{непр}$ указывают в эксплуатационной документации. При отсутствии данных в документации системы используют статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные.

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ корр}$ и условие α. Условие α касается обеспечения корректности обработки информации и формулируется в виде ограничений: $P_{корр} \geq P_{доп\ корр}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента корректности обработки информации в системе $Z_{корр}$

$$Z_{корр} = \begin{cases} 1, \text{ если условие обеспечения корректности обработки информации } \alpha \text{ выполнено,} \\ P_{корр}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.26)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{корр})$ в качестве вероятностного выражения риска нарушения корректности обработки информации в системе.

В.3.8 Модели для оценки безошибочности действий пользователей и персонала системы

Модель позволяет оценить воздействие «человеческого фактора» на уровне вероятности безошибочных действий пользователей и персонала системы в течение заданного периода прогноза $P_{чел}(T_{зад})$.

Требуемая безошибочность действий пользователей и персонала системы в течение заданного времени обеспечивается на основе профессионального отбора, специальной подготовки пользователей и обслуживающего персонала системы, реализации и использования эффективных средств программной поддержки. Безошибочность является следствием приемлемого соотношения между частотой возможных ошибок, временем их обнаружения и исправления.

С точностью до переопределений исходных данных для расчета вероятности безошибочных действий пользователей и персонала системы в течение заданного периода прогноза используют математические модели В.2, В.3.2, В.3.6, В.3.7 или аналогичные им с учетом специфики действий — см. способ 1 из В.2.4, а также ГОСТ Р 59333.

Для системного анализа результатов моделирования в оценках интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации (см. В.3.10) задают допустимый уровень $P_{доп\ чел}(T_{зад})$ и условие α. Условие α касается безошибочности действий пользователей и персонала системы и формулируется в виде ограничений: $P_{чел}(T_{зад}) \geq P_{доп\ чел}(T_{зад})$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочных действий пользователей и персонала системы $Z_{чел}(T_{зад})$

$$Z_{чел}(T_{зад}) = \begin{cases} 1, \text{ если условие безошибочности действий } \alpha \text{ выполнено,} \\ P_{чел}(T_{зад}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases} \quad (В.27)$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы этого коэффициента $[1 - Z_{чел}(T_{зад})]$ в качестве вероятностного выражения риска нарушения безошибочности действий пользователей и персонала системы.

В.3.9 Адаптация моделей В.2 к модели угроз

В.3.9.1 Общие положения

В общем случае для прогнозирования рисков нарушения требований по защите информации используют модели В.2. Вместе с тем при необходимости детализации влияния угроз на сохранение целостности, доступности и/или конфиденциальности информации с учетом описательного характера модели угроз безопасности информации возможна адаптация математических моделей В.2.

Приводимые в В.3.9.2 — В.3.9.4 модели представляют собой примеры типовой адаптации для оценки:

- сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий;
- защищенности активов от несанкционированного доступа;
- сохранения конфиденциальности используемой информации.

В.3.9.2 Модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий

Модель позволяет оценить вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $P_{возд}(T_{зад})$.

Под моделируемой системой понимается отдельное действие или множество действий процесса, выполняемых с использованием определенных защищаемых активов, в условиях опасных программно-технических воздействий. Для каждого из анализируемых действий возможно либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения этого действия. В результате математического моделирования рассчитывают вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза в течение всего периода прогноза. Ее дополнение до единицы представляет собой веро-

ятность нарушения целостности моделируемой системы (в частности, защищаемых активов) в условиях опасных программно-технических воздействий. В свою очередь эта последняя вероятность в сопоставлении с возможным ущербом определяет риск нарушения целостности моделируемой системы (в частности, защищаемых активов) в течение заданного периода прогноза.

В.3.9.2.1 Математическая модель для прогнозирования риска при отсутствии какого-либо контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением формализации по модели В.2.2. Специфика состоит в логическом переопределении исходных данных для моделирования (см. В.3.9.2.2 и приложение Г). Это означает применение способа 1 из В.2.4. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности моделируемой системы в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели является расчетный риск нарушения целостности выполняемых действий процесса управления информацией системы в условиях опасных программно-технических воздействий в течение заданного периода прогноза при отсутствии какого-либо контроля. Применимы методы повышения адекватности по В.2.4.

Модель применяют для случая, когда в системе отсутствует какой-либо контроль (диагностика) целостности реализуемых действий процесса. Модель представляет собой частный случай моделей В.2.3 и В.3.9.2.2, если период между диагностиками целостности моделируемой системы больше периода прогноза.

В.3.9.2.2 Математическая модель для прогнозирования риска при реализации технологии периодического системного контроля

Моделируемая система представлена в виде «черного ящика» с полным повторением математической формализации по модели В.2.3. Специфика состоит в логическом переопределении исходных данных для моделирования — см. способ 1 из В.2.4, а также приложение Г. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности моделируемой системы в течение заданного периода прогноза. С точки зрения системной инженерии результатом применения модели является расчетный риск нарушения выполняемых действий процесса управления информацией системы в условиях опасных программно-технических воздействий в течение заданного периода прогноза при реализации технологии периодического системного контроля. Применимы методы повышения адекватности по В.2.4.

Для расчета риска нарушения реализации процесса управления информацией системы в условиях опасных программно-технических воздействий выполняют адаптацию исходных данных применительно к выполняемым действиям процесса и защищаемым активам:

σ — частота возникновения источников угроз в виде источников опасных программно-технических воздействий на моделируемую систему;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса или защищаемых активов, используемых при выполнении действия) в результате опасных программно-технических воздействий;

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

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

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

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

Примечание — Несмотря на фактическую повторяемость названий исходных данных, их значения при моделировании по модели В.3.9.2.2 будут отличны от значений при моделировании по модели В.2, поскольку различны их природа, исходные данные, интерпретация и области приложений. Соответственно разными будут и расчетные риски по этим моделям.

В итоге вероятность $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ отсутствия нарушений целостности моделируемой системы в течение периода прогноза $T_{зад}$ определяется теми же аналитическими выражениями (В.2) — (В.9), что и в моделях В.2.3, В.2.4, в зависимости от варианта соотношений между исходными данными.

Сопоставление с возможным ущербом позволяет также рассматривать рассчитываемую по формуле (В.1) вероятность нарушения требований по защите информации в моделируемой системе $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ в качестве риска нарушения выполняемых действий процесса управления информацией в системе в условиях опасных программно-технических воздействий в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления целостности моделируемой системы.

В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель В.3.9.2.2 превращается в модель В.3.9.2.1 для прогнозирования риска при отсутствии какого-либо контроля.

Необходимые границы исходных значений программно-технических угроз для моделируемой системы задаются в ТЗ или в постановках функциональных задач системы при указании сценариев возможного опасного воздействия, длительность диагностики устанавливают в результате натурных экспериментов, а значение периода между контролями (диагностиками) указывают в эксплуатационной документации. При отсутствии данных в документации системы используют статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные.

В.3.9.3 Модель для оценки защищенности активов от несанкционированного доступа

Модель позволяет оценить вероятность обеспечения защищенности активов системы от НСД в течение заданного периода прогноза $P_{НСД}(T_{зад})$ или без привязки к этому периоду $P_{НСД}$.

Примечания

1 Под нарушителем безопасности информации может выступать, например, программная закладка или субъект, совершивший действие (случайно или преднамеренно), следствием которого является возникновение и/или реализация угроз нарушения безопасности информации в системе.

2 Под нарушителем правил разграничения доступа понимается субъект доступа, осуществляющий несанкционированный доступ к информации, например, преступные группы и сообщества, иные нарушители, в т. ч. из состава пользователей и персонала системы. Они имеют мотивацию, достаточные компетенции для НСД и обладают необходимой технической оснащенностью. Это позволяет им изменять значения критически важных параметров процессов функционирования системы (включая серверы, рабочие места операторов, контроллеры управления).

Требуемую защищенность активов системы от НСД обеспечивают на основе реализации достаточного количества защитных преград потенциальным угрозам и различным нарушителям, выбора относительно стойких к вскрытию средств и алгоритмов защиты и рациональной смены параметров защиты. Предполагают, что НСД к ресурсам состоялся, когда все преграды преодолены. Преграду считают преодоленной, если время, затраченное на ее преодоление, оказывается меньше времени между соседними изменениями защитных параметров преграды.

В общем случае в предположении независимости преодолеваемых преград вероятность сохранения защищенности активов системы от НСД вычисляют по формуле

$$P_{НСД} = 1 - \prod_{m=1}^{M} P_{преод\ m}, \qquad (В.28)$$

где M — количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

$P_{преод\ m}$ — вероятность преодоления нарушителем m-й преграды.

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости вероятность преодоления нарушителем m-й преграды $P_{преод\ m}$ без привязки к периоду прогноза вычисляют по формуле

$$P_{преод\ m} = \frac{f_m}{f_m + u_m}, \qquad (В.29)$$

где f_m — среднее время между соседними изменениями параметров защиты m-й преграды;

u_m — среднее время преодоления (вскрытия значений параметров защиты) m-й преграды.

С учетом специфики расчет $P_{преод\ m}$ для отдельной m-й преграды или для всех M преград может быть осуществлен с использованием модели В.2 (m – 1, ..., M). В этом случае будет иметь место зависимость рассчитываемого показателя от задаваемого периода прогноза $T_{зад\ m}$, т. е. $P_{преод\ m}(T_{зад\ m}) = 1 - P_{возд\ m}(T_{зад\ m})$, где вероятность отсутствия опасного воздействия в результате НСД $P_{возд\ m}(T_{зад\ m})$ вычисляют по формулам (В.2) — (В.9), т. е. $P_{возд\ m}(T_{зад\ m}) = P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад\ m})$. В такой адаптации возможна комбинация вышеуказанных моделей. Тогда в выражении (В.28) в соответствующих сомножителях $P_{преод\ m}(T_{зад\ m})$ может быть привязка к задаваемому периоду прогноза $T_{зад\ m}$, и тогда рассчитываемая вероятность обеспечения защищенности активов системы от НСД $P_{НСД}(T_{зад})$ также будет зависеть от задаваемых периодов прогноза $T_{зад\ m}$ (для тех преград, для которых осуществляется расчет по моделям В.2). Причем задаваемые в расчетах периоды прогноза $T_{зад\ m}$ для m-й преграды выбирают таким образом, чтобы их сумма для всех M преград не превышала общей длительности задаваемого периода прогноза для системы $T_{зад}$.

Необходимые для моделирования исходные данные по количеству преград M и границам значений u_m определяют в результате дополнительного моделирования, натурных экспериментов, учитывающих специфику системы защиты и возможные сценарии действий нарушителей, или сравнения с аналогами. Их указывают в конструкторской документации в приложении к возможным сценариям НСД, конкретизирующим требования ТЗ в части обеспечения информационной безопасности, а значения f_m — в эксплуатационной документации. При отсутствии данных в документации системы используют статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные, включая данные для моделей В.2.

В.3.9.4 Модель для оценки сохранения конфиденциальности используемой информации

Модель позволяет оценить вероятность $P_{конф}(T_{конф})$ сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $T_{конф}$.

Под конфиденциальностью информации в моделируемой системе понимается свойство используемой информации быть сохраненной в течение заданного объективного периода конфиденциальности $T_{конф}$ от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими или программными средствами.

Примечание — Сохраняют силу определения, принятые в рамках модели В.3.9.3.

Требуемая конфиденциальность информации в системе обеспечивается на основе реализации мероприятий, гарантирующих защищенность активов от НСД (см. модель В.3.9.3) до истечения периода объективной конфиденциальности данной информации для ее использования.

Вероятность сохранения конфиденциальности используемой информации вычисляют по формуле (В.28) с тем отличием, что M — это количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к информации, а $P_{\text{преод }m}$ — вероятность преодоления нарушителем m-й преграды до истечения периода объективной конфиденциальности используемой информации $T_{\text{конф}}$. Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости $P_{\text{преод }m}$ в этом случае вычисляют по формуле

$$P_{\text{преод }m} = \frac{T_{\text{конф}} f_m}{T_{\text{конф}} f_m + u_m f_m + u_m T_{\text{конф}}}, \tag{В.30}$$

где f_m, u_m определены в модели В.3.9.3.

Примечание — Конфиденциальность информации может быть нарушена, например, в результате противоправных действий допущенных к ней лиц в форме разглашения защищаемой информации, когда ни одну преграду преодолевать не приходится. В этом случае в качестве виртуальной сдерживающей преграды (возможно, нескольких преград) могут быть рассмотрены принятые обязательства о неразглашении защищаемой информации и установленная персональная ответственность в виде возможного наказания.

Необходимые для моделирования исходные значения M, где f_m, u_m устанавливают так же, как и для модели В.3.9.3, диапазон возможных значений $T_{\text{конф}}$ указывают в ТЗ или в постановках функциональных задач. При отсутствии данных в документации системы используют статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные, включая данные для моделей В.2.

При больших значениях $T_{\text{конф}}$ формула (В.30) вырождается в формулу (В.29).

Примечание — При проведении системного анализа период объективной конфиденциальности используемой информации $T_{\text{конф}}$ может играть роль задаваемого периода прогноза $T_{\text{зад}}$, и наоборот — задаваемый период прогноза $T_{\text{зад}}$ может играть роль периода объективной конфиденциальности $T_{\text{конф}}$. В такой адаптации возможна комбинация вышеуказанных моделей. С учетом специфики расчет для некоторых из преград (в частности для m-й преграды — это показатель $P_{\text{преод }m}(T_{\text{зад }m})$ — вероятность преодоления нарушителем m-й преграды до истечения задаваемого периода прогноза $T_{\text{зад }m}$) может быть осуществлен с использованием моделей В.2. В этом случае $P_{\text{преод }m}(T_{\text{зад }m}) = 1 - P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад }m})$ где вероятность отсутствия опасного воздействия в результате НСД $P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад }m})$ вычисляют по формулам (В.2) — (В.9).

В.3.10 Алгоритм расчета интегрального риска нарушения реализации процесса с учетом требований по защите информации

Показатель интегрального риска позволяет оценить свойства процесса управления информацией в системе сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях реализации с обеспечением надежности и своевременности предоставления, полноты, достоверности и безопасности используемой информации и соблюдением требований по защите информации. Интегральный риск используют для сравнения весомости прогнозируемых частных рисков, выявления явных и скрытых угроз и поддержки принятия решений для задач системного анализа.

В сопоставлении с возможным ущербом интегральный риск нарушения реализации процесса управления информацией системы с учетом требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$ для прогнозного периода $T_{\text{зад}}$ определяют по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - [1 - R_{\text{надежн}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})], \tag{В.31}$$

где $R_{\text{надежн}}(T_{\text{зад}})$ — вероятность нарушения надежности реализации процесса управления информацией системы в течение периода прогноза $T_{\text{зад}}$ без учета требований по защите информации, рассчитывается по моделям и рекомендациям В.3.2—В.3.8;

$R_{\text{наруш}}(T_{\text{зад}})$ — вероятность нарушения требований по защите информации в системе для процесса управления информацией в течение периода прогноза $T_{\text{зад}}$, рассчитывается по моделям и рекомендациям В.2.

Вероятность нарушения надежности реализации процесса управления информацией системы в течение периода прогноза без учета требований по защите информации $R_{\text{надежн}}(T_{\text{зад}})$ определяют как дополнение до единицы вероятности того, что процесс управления информацией системы обеспечивает надежность и своевременность предоставления запрашиваемой или выдаваемой принудительно информации, полноту, достоверность используемой информации и безошибочность действий пользователей и персонала (учитывая возможные ограничения на расчетные вероятностные показатели), т. е.

$$R_{\text{надежн}}(T_{\text{зад}}) = 1 - Z_{\text{над предст}}(T_{\text{зад}}) \cdot Z_{\text{своевр}} \cdot Z_{\text{полн}} \cdot Z_{\text{акт}} \cdot Z_{\text{безош}} \cdot Z_{\text{корр}} \cdot Z_{\text{чел}}(T_{\text{зад}}), \tag{В.32}$$

где $Z_{\text{над предст}}(T_{\text{зад}})$ — вероятностный коэффициент надежности предоставления информации, учитывающий вероятность надежного предоставления информации в системе в течение заданного периода прогноза $T_{\text{зад}}$ и соответствующие условия α, определяется по модели В.3.2;

$Z_{\text{своевр}}$ — вероятностный коэффициент своевременности обработки запросов, учитывающий относительную долю своевременно обработанных в системе запросов и соответствующие условия α, определяется по модели В.3.3;

$Z_{\text{полн}}$ — вероятностный коэффициент полноты оперативного отражения в системе новых объектов и явлений, учитывающий вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений, и соответствующие условия α, определяется по модели В.3.4;

$Z_{\text{акт}}$ — вероятностный коэффициент актуальности информации в системе, учитывающий вероятность сохранения актуальности информации на момент ее использования и соответствующие условия α, определяется по модели В.3.5;

$Z_{\text{безош}}$ — вероятностный коэффициент безошибочности информации в системе, учитывающий вероятность отсутствия ошибок в информации после ее контроля и соответствующие условия α, определяется по модели В.3.6;

$Z_{\text{корр}}$ — вероятностный коэффициент корректности обработки информации в системе, учитывающий вероятность получения корректных результатов обработки информации и соответствующие условия α, определяется по модели В.3.7;

$Z_{\text{чел}}(T_{\text{зад}})$ — вероятностный коэффициент безошибочных действий пользователей и персонала системы, учитывающий вероятность безошибочных действий пользователей и персонала в течение заданного периода прогноза и соответствующие условия α, определяется по модели В.3.8.

В общем случае вероятность нарушения требований по защите информации в системе для процесса управления информацией в течение периода прогноза $R_{\text{наруш}}(T_{\text{зад}})$ определяют по моделям В.2. В конкретных случаях при необходимости детализации модели угроз безопасности информации для учета защищенности от опасных программно-технических воздействий, от НСД, сохранения конфиденциальности информации применяют аналитическую адаптацию моделей. При этом вероятность $R_{\text{наруш}}(T_{\text{зад}})$ определяют по формуле

$$R_{\text{наруш}}(T_{\text{зад}}) = 1 - P_{\text{возд}}(T_{\text{зад}}) \cdot P_{\text{НСД}}(T_{\text{зад}}) \cdot P_{\text{конф}}(T_{\text{конф}}), \quad \text{(В.33)}$$

где $P_{\text{возд}}(T_{\text{зад}})$ — вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $T_{\text{зад}}$, определяемая по рекомендациям В.3.9.2 как $P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$;

$P_{\text{НСД}}(T_{\text{зад}})$ — вероятность обеспечения защищенности активов системы от НСД в течение заданного периода прогноза $T_{\text{зад}}$ (или без привязки к этому периоду — $P_{\text{НСД}}$), определяемая по рекомендациям В.3.9.3;

$P_{\text{конф}}(T_{\text{конф}})$ — вероятность сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $T_{\text{конф}}$, определяемая по рекомендациям В.3.9.4 (период $T_{\text{конф}}$ может играть роль периода прогноза $T_{\text{зад}}$ — см. последнее примечание в 3.9.4).

Приложение Г
(справочное)

Методические указания по прогнозированию рисков для процесса управления информацией системы

Г.1 Общие положения

Г.1.1 Настоящие методические указания охватывают типовые действия при прогнозировании основных количественных показателей рисков:

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

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

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

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

Г.1.3 Для прогнозирования рисков определению подлежат:

- состав выходных результатов и выполняемых действий процесса управления информацией системы и используемых при этом активов;
- перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для выходных результатов, выполняемых действий процесса управления информацией системы и используемых при этом активов;
- технологии противодействия угрозам, используемые в процессе управления информацией системы в заданной среде ее применения;
- формализованные требования к качеству информации, используемой в системе (включая требования к надежности и своевременности представления запрашиваемой и выдаваемой принудительно информации, полноте, достоверности и безопасности используемой информации).

Примечание — Для более детального понимания специфики системы при прогнозировании рисков см., например, ГОСТ Р 58494, где в приложении к системе дистанционного контроля промышленной безопасности в опасном производстве указаны примеры объектов, выходных результатов, выполняемых действий, перечень потенциальных угроз.

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

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

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

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

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

Г.2 Цель прогнозирования рисков

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

Г.3 Положения по формализации

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

Г.3.2 Для каждого из элементов моделируемой системы в зависимости от поставленных целей могут решаться свои задачи системного анализа (см. раздел 7). В общем случае моделируемую систему представляют либо в виде «черного ящика» (см. В.2.2 и В.2.3, В.3.1 — В.3.9), либо в виде сложной системы, элементы которой объединяются последовательно или параллельно (см. В.2.4, В.3.10). 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 ее целевому назначению. Примеры декомпозиции сложной системы до составных элементов представлены на рисунках Г.1, Г.2. Для каждого элемента могут оказаться характерными свои разнородные угрозы и применяемые технологии контроля и восстановления нарушаемой целостности.



Рисунок Г.1 — Пример моделируемой системы, представляющей собой множество выходных результатов. Системный элемент — конкретный выходной результат (всего / элементов)



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

Г.3.3 Для каждого из составляющих элементов и для моделируемой системы в целом вводится пространство элементарных событий (состояний) с учетом логических взаимосвязей элементов условиями «И», «ИЛИ».

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

- «Выполнение требований по защите информации в процессе управления информацией системы обеспечено», если в течение всего периода прогноза обеспечено выполнение определенных требований по защите информации, т. е. с точки зрения математического моделирования их невыполнение способно привести к недопустимому ущербу;
- «Выполнение требований по защите информации в процессе управления информацией системы нарушено» — в противном случае.

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

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

Г.3.4 В общем случае с применением 1-го способа по В.2.4 возможно расширение или переименование самих элементарных событий (состояний), главное, чтобы они формировали полное множество аналогично множествам, приведенным в настоящем подразделе в качестве примеров.

В Г.7 приведены демонстрационные примеры прогнозирования рисков и решения некоторых вопросов системного анализа с использованием получаемых результатов прогнозирования.

Г.4 Показатели, исходные данные и расчетные соотношения

Применительно к моделируемой системе, которая может быть представлена в виде «черного ящика» (см. В.2.2, В.2.3, В.3) или сложной логической структуры (см. В.2.4, В.3), расчетными показателями являются:

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

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

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

Применительно к моделируемой системе исходными данными являются данные, необходимые для проведения расчетов по моделям и рекомендациям В.2, В.3.

Г.5 Порядок прогнозирования рисков

Для прогнозирования рисков осуществляют следующие шаги.

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

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

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

Шаг 4. Выбирают расчетные показатели (см. Г.4). Выбирают подходящие математические модели и методы повышения их адекватности из В.2, В.3. Разрабатывают необходимые методики системного анализа, обеспечивающие более детальный учет особенностей процесса управления информацией системы (см. приложение Е). Осуществляют расчет выбранных показателей с использованием соответствующих соотношений (В.1) — (В.33) и иных рекомендаций приложения В.

Шаг 5. Результаты расчетов применяют для достижения поставленных целей (см. Г.2).

Г.6 Обработка и использование результатов прогнозирования рисков

Результаты прогнозирования рисков должны быть удобны для обработки заказчиком системного анализа и/или аналитиком моделируемой системы. Результаты расчетов представляются в виде гистограмм, графиков и/или 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, Г.2, приложение Е и ГОСТ Р 59349.

Г.7 Примеры

Г.7.1 Приведенные примеры демонстрируют отдельные аналитические возможности методических указаний. Пусть руководство некоторой угольной шахты, предпринимая меры по управлению информацией для совершенствования бизнеса, повышения уровня промышленной и информационной безопасности производства (см. [1] — [3], [9] — [12], [15] — [17]) приняло решение о создании СДК. Именно СДК далее будет позиционироваться как моделируемая система в рамках процесса управления информацией. В общем случае применение СДК нацелено на оперативное выявление и оповещение ответственных лиц о предпосылках возникновения либо о возникновении опасных ситуаций на производственных объектах, удаленную информационно-аналитическую поддержку в интересах обеспечения нормальных условий функционирования производственных объектов и реализации на предприятиях риск-ориентированного подхода. Такие сущности, как охваченные дистанционным контролем объекты и непосредственно процессы функционирования СДК (обеспечивающие качество используемой информации) характеризуют моделируемые в примерах системы.

С учетом возможных ущербов цели прогнозирования рисков сформулированы руководством шахты следующим образом:

- количественно определить критичные условия в процессе управления информацией СДК;
- выработать рекомендации по обеспечению нормальных условий функционирования опасных производственных объектов на основе рационального применения СДК;

Тем самым выполнены шаги 1, 2 настоящих методических указаний.

Нижеследующие примеры посвящены оценке свойств процесса управления информацией системы, характеризующих способность выполнить процесс в заданных условиях реализации с обеспечением надежности и своевременности предоставления, полноты, достоверности и безопасности используемой информации и соблюдением требований по защите информации в СДК.

Шаги 3, 4 и 5 настоящей методики выполняются далее в рамках каждого из примеров.

Учитывая, что риск нарушения требований по защите информации является составной частью интегрального риска, демонстрация примеров проведена в последовательности, соответствующей последовательности расчетных показателей, приведенных в моделях В.3. В примерах 1—10 (см Г.7.2 — Г.7.11) продемонстрированы подходы к оценке:

- вероятности надежного предоставления информации в системе в течение заданного периода прогноза $P_{\text{над предст}}(T_{\text{зад}})$, определяемой по модели В.3.2;
- относительной доли своевременно обработанных запросов тех типов, для которых выполняются требования по своевременности $C_{\text{своевр}}$, определяемой по модели В.3.3;
- вероятности того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{\text{полн}}$, определяемой по модели В.3.4;
- вероятности сохранения актуальности информации на момент ее использования $P_{\text{акт}}$, определяемой по модели В.3.5;
- вероятности отсутствия ошибок в информации после ее контроля $P_{\text{безош}}$, определяемой по модели В.3.6;
- вероятности получения корректных результатов обработки информации $P_{\text{корр}}$, определяемой по модели В.3.7;
- вероятности безошибочных действий пользователей и персонала системы в течение заданного периода прогноза $P_{\text{чел}}(T_{\text{зад}})$, определяемой по модели В.3.8;
- вероятности отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $P_{\text{возд}}(T_{\text{зад}})$, определяемой по модели В.3.9.2;
- вероятности обеспечения защищенности активов системы от НСД $P_{\text{НСД}}$, определяемой по модели В.3.9.3;
- вероятности сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $P_{\text{конф}}(T_{\text{конф}})$, определяемой по модели В.3.9.4.

В последнем примере (пример 11, см. Г.7.12) эти результаты используются для расчета интегрального риска нарушения реализации процесса управления информацией с учетом требований по защите информации по формулам из В.3.10.

Г.7.2 Пример 1 демонстрирует подход к оценке вероятности надежного предоставления информации в СДК в течение заданного периода прогноза $P_{\text{над предст}}(T_{\text{зад}})$.

Объектами анализа являются комплекс главных вентиляторных установок, комплекс модульных дегазационных установок и газоотсасывающая установка шахты, охваченные функциональными возможностями СДК и являющиеся источниками информации для последующей обработки и использования по назначению (см. структуру сложной моделируемой системы на рисунке Г.3). Возможные ущербы при отказах оборудования в моделируемой системе связаны:

- с опасностью аварии из-за возгорания метана и возможного пожара на шахте;
- с простоями производства, что ведет к недополучению дохода предприятия из-за вынужденных простоев шахты.

Надежность предоставления используемой информации на шахте определяется надежностью функционирования средств СДК совместно с контролируемым оборудованием. Это означает, что надежность предоставления информации в СДК должна быть выше, чем надежность функционирования контролируемого оборудования.

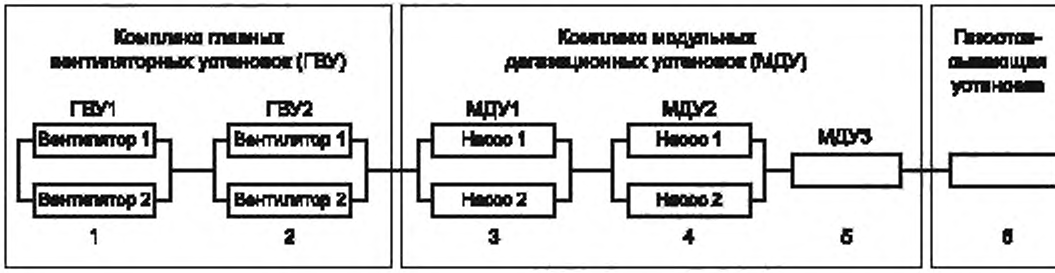


Рисунок Г.3 — Моделируемая система, логически структурированная до составных объектов анализа, охваченных функциональными возможностями СДК

Логическая интерпретация событий для моделируемой системы следующая: надежность функционирования моделируемой системы обеспечена, когда обеспечена надежность функционирования объектов, охваченных функциональными возможностями СДК:

- «И» ГВУ (в том числе ГВУ 1 «И» ГВУ 2), имеющих различное местоположение в комплексе ГВУ и отличающихся характеристиками по безотказности;
- «И» МДУ (в том числе «И» МДУ 1, «И» МДУ 2, «И» МДУ 3), также имеющих различное местоположение в комплексе МДУ и отличающихся характеристиками по безотказности;
- «И» газоотсасывающей установки,

В свою очередь каждая из ГВУ (т. е. ГВУ 1 и ГВУ 2) находится в работоспособном состоянии (т. е. признается функционирующей надежно), если «ИЛИ» вентилятор 1, «ИЛИ» вентилятор 2 находится в работоспособном состоянии (это достигается резервированием вентиляторов). Каждая из МДУ (т. е. МДУ 1 и МДУ 2) находится в работоспособном состоянии (т. е. признается функционирующей надежно), если «ИЛИ» насос 1, «ИЛИ» насос 2 в их составе находится в работоспособном состоянии (это достигается резервированием насосов). В МДУ 3 резервный насос отсутствует (см. рисунок Г.3).

Исходные данные для моделирования отражены в таблице Г.1.

Таблица Г.1 — Исходные данные для оценки вероятности надежного предоставления информации в СДК в течение заданного периода прогноза

Исходные данные	Значения и комментарии					
	Комплекс ГВУ		Комплекс МДУ			Газоотсасывающая установка
	ГВУ 1 (для каждого вентилятора)	ГВУ 2 (для каждого вентилятора)	МДУ 1 (для каждого насоса)	МДУ 2 (для каждого насоса)	МДУ3	
σ — частота возникновения источников угроз (например, выхода значений контролируемых параметров за границы рабочего диапазона)	1 раз в месяц	1 раз в 2 месяца (т. е. безотказность каждого вентилятора в 2 раза выше по сравнению с ГВУ 1)	1 раз в 3 месяца (т. е. безотказность каждого насоса в 3 раза выше по сравнению с ГВУ 1)	1 раз в 6 месяцев (т. е. безотказность каждого насоса в 2 раза выше по сравнению с МДУ 1)	1 раз в год (т. е. в 4 раза выше по сравнению с МДУ 1)	1 раз в 2 года (т. е. в 24 раза выше по сравнению с ГВУ 1 и в 8 раз выше по сравнению с МДУ 1)
β — среднее время развития угроз с момента возникновения источников угроз до нарушения (например, выхода значений контролируемых параметров за границы нормативного диапазона)	30 минут (оценка среднего времени до возгорания метана после отказа ГВУ, МДУ или газоотсасывающей установки)					
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики	5 минут (с учетом переключения внимания диспетчера на выполнение разных функций)					
$T_{диаг}$ — среднее время диагностики	1 минута (включая необходимую отдачу распоряжений)					
$T_{восст}$ — среднее время восстановления после выявления нарушений	20 минут (оценка среднего времени реакции ответственного лица на сигналы СДК о предпосылках возникновения опасных ситуаций)					
$T_{зад}$ — задаваемая длительность периода прогноза	1 месяц (период времени, в течение которого возможно принятие упреждающих мер, направленных на поддержание рисков в допустимых пределах)					

Моделирование осуществлено с использованием модели В.3.2.

Системный анализ результатов расчетов показал, что при ориентации на надежность функционирования всех составных элементов моделируемой системы (ГВУ 1, 2, МДУ 1, 2, 3 и газоотсасывающей установки) нижняя оценка вероятности надежного предоставления информации в СДК в течение месяца за все оборудование равна $P_{над\ предст}(T_{зад}) = 0{,}786$ (см. рисунок Г.4).

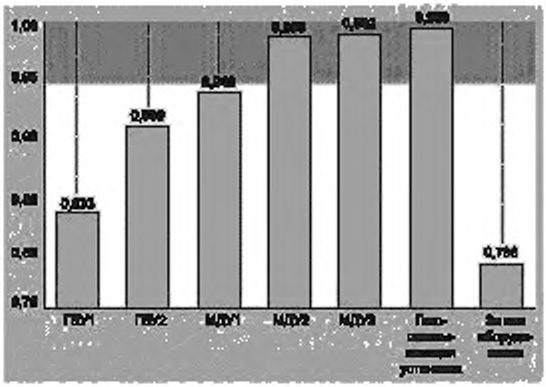


Рисунок Г.4 — Оценки для вероятности надежного предоставления информации в СДК в течение месяца за все оборудование и поэлементно: за ГВУ 1, 2, МДУ 1, 2, 3 и газоотсасывающую установку

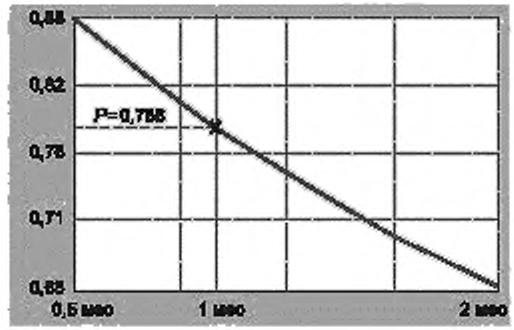


Рисунок Г.5 — Зависимость вероятности надежного предоставления информации в СДК (за все оборудование) от периода прогноза длительностью от 0,5 месяца до 2 месяцев

Узким местом является надежность функционирования главной вентиляторной установки ГВУ 1. Это объясняется тем, что при прочих равных условиях наработка вентиляторов ГВУ 1 на отказ составляет 1 месяц, что в разы меньше аналогичной наработки на отказ для вентиляторов ГВУ 2, насосов модульных дегазационных установок МДУ 1, 2, 3 и газоотсасывающей установки.

В свою очередь анализ зависимости вероятности надежного предоставления информации в СДК от периода прогноза (см. рисунок Г.5) позволяет обосновать рекомендацию: сроки планирования и реализации мер, связанных с поддержанием надежности функционирования средств СДК не должны превышать двух недель, при этом среднее время диагностики с использованием СДК должно быть не более 1 мин, а среднее время реакции ответственного лица на сигналы СДК о предпосылках возникновения опасных ситуаций не должно превышать 20 мин. В этом случае вероятность надежного предоставления информации превысит 0,88, что более, чем в 7 раз превысит вероятностное значение риска нарушения надежности [0,88/(1 – 0,88) = 7,3].

Для расчета интегрального риска в примере 11 при ограничениях на вероятность надежного предоставления информации в СДК не ниже 0,95 коэффициент надежности предоставления информации $Z_{\text{над предст}}(T_{\text{зад}})$ также будет равен $P_{\text{над предст}}(T_{\text{зад}}) = 0{,}786$, т. е. $Z_{\text{над предст}}(T_{\text{зад}}) = 0{,}786$.

Г.7.3 Пример 2 поясняет логику подхода к оценке относительной доли своевременно обработанных запросов лишь тех типов, для которых выполняются требования по своевременности $C_{\text{своевр}}$.

Объектами анализа являются информационные запросы и их временные задержки при обработке в СДК для предоставления необходимой информации пользователям в режиме реального времени функционирования шахты.

На этапе проектирования СДК осуществляется поиск эффективных путей реализации функциональных возможностей по сбору данных о состоянии промышленной безопасности, выработке решений и планированию мер противодействия угрозам, контролю и оповещению. Требования к своевременности предоставления выходной информации с использованием СДК диктуются состоянием промышленной безопасности, а также требованиями функционирования СДК в режиме реального времени.

При этом должна быть обеспечена своевременность ввода информации в БД и своевременное предоставление выходной информации для ее последующего использования по назначению. Для обеспечения возможности оценки своевременности предоставления используемой информации согласно модели В.3.3 требования для 10 типов информации ($i = 1,\ldots,10$) сформулированы следующим образом:

- $i = 1$ — время автоматического ввода в БД поступившей исходной оперативной информации от источников, а также время выдачи контрольной технологической информации о состоянии контролируемого оборудования и самой СДК с вероятностью не ниже 0,95 не должно превышать 10 с, т. е. для $i = 1$ $P_{\text{св }1}(\tau_1 \le 10\text{ с}) \ge 0{,}95$;

- $i = 2$ — время отображения на экране мониторов пользователей команд, приказов и срочных сигналов, поступивших в СДК, с вероятностью не ниже 0,9 не должно превышать 10 с, т. е. для $i = 2$ $P_{\text{св }2}(\tau_2 \le 10\text{ с}) \ge 0{,}9$;

- $i = 3$ — время ввода в БД другой оперативной исходной информации от источников с вероятностью не ниже 0,8 не должно превышать 30 с, т. е. для $i = 3$ $P_{\text{св }3}(\tau_3 \le 30\text{ с}) \ge 0{,}8$;

- $i = 4$ — время начала предоставления результатов с момента запроса на решение информационно-аналитических задач с вероятностью не ниже 0,8 не должно превышать 1 мин 20 с, т. е. для $i = 4$ $P_{\text{св }4}(\tau_4 \le 1\text{мин }20\text{ с}) \ge 0{,}8$;

- $i = 5$ — время начала предоставления подробных справок с момента запроса при работе с электронно-пространственными модели на шахте с вероятностью не ниже 0,7 не должно превышать 1 мин 40 с, т. е. для $i = 5$ $P_{\text{св }5}(\tau_5 \le 1\text{ мин }40\text{ с}) \ge 0{,}7$;

- i = 6 — время обработки запросов при выполнении общесистемных функций СДК с момента задания аналитических расчетов до начала выдачи результатов с вероятностью не ниже 0,7 не должно превышать 2 мин 30 с, т. е. для i = 6 $P_{св\ 6}$ ($\tau_6 \le$ 2 мин 30 с) ≥ 0,7;

- i = 7 — время прогнозных расчетов при планировании мер противодействия угрозам в работе оборудования шахты с вероятностью не ниже 0,7 не должно превышать 4 мин, т. е. для i = 7 $P_{св\ 7}$ ($\tau_7 \le$ 4 мин) ≥ 0,7;

- i = 8 — время оперативных статистических отчетов СДК с момента задания до начала выдачи результатов не должно превышать в среднем 2,5 мин, т. е. для i = 8 $T_{полн\ 8} \le$ 2,5 мин;

- i = 9 — время ввода в БД информации по контролю и управлению функционированием СДК не должно превышать в среднем 3 мин, т. е. для i = 9 $T_{полн\ 9} \le$ 3 мин;

- i = 10 — время решения задач и подготовки отчетов по обеспечению информационной безопасности СДК с момента задания до начала выдачи результатов не должно превышать в среднем 3 мин, т. е. для i = 10 $T_{полн\ 10} \le$ 3 мин.

Для оценки предъявленных требований по своевременности обработки указанных типов информации СДК проводят измерения согласно модели В.3.3. При этом для расчета вероятностно-временных показателей могут быть использованы другие математические модели систем массового обслуживания. Учитывают временные задержки для типовой загрузки (или при необходимости — для наивысшей загрузки) вычислительных средств и средств связи СДК. Определяют среднее время и среднеквадратичное отклонение времени реакции системы при обработке указанных типов информации. Вероятность своевременной обработки оценивают по формуле (В.11), а относительную долю своевременно обработанных в системе запросов лишь тех типов, для которых выполнены требования заказчика по установленным критериям своевременности обработки, оценивают по формуле (В.12). Значения возможных результатов измерений T_i и оценки $P_{св\ i}$ ($T_{зад\ i}$) приведены соответственно на рисунках Г.6 и Г.7.

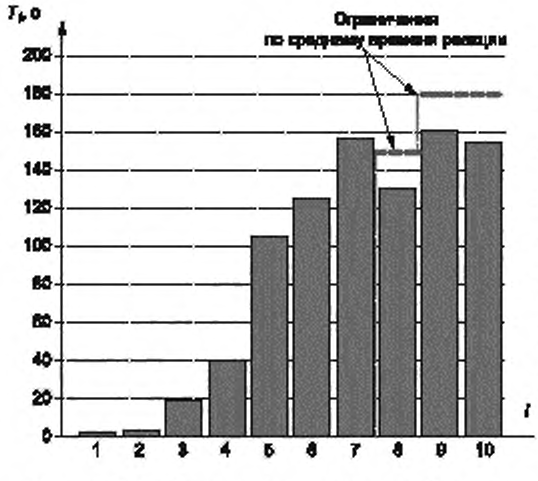


Рисунок Г.6 — Среднее время реакции по 10 типам информации

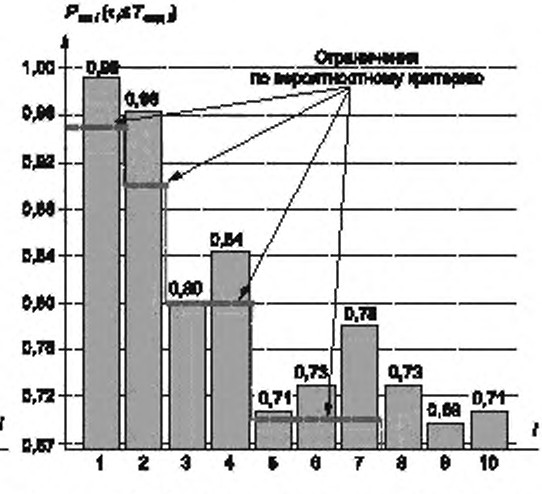


Рисунок Г.7 — Вероятность своевременной обработки 10 типов информации

Если для простоты понимания в рамках примера 2 частота поступления на обработку запросов каждого из 10 типов одинакова, то, учитывая, что все требования к своевременности выполнены (для типов i = 1, ...,7 — по вероятностному критерию, для типов i = 8, 9, 10 — по среднему времени реакции), относительная доля своевременно обработанных запросов $C_{своевр}$ составляет по формуле (В.12) десятую часть от суммы вероятностей своевременной обработки всех 10 типов информации (т.к. все $\lambda_i = \lambda$), т. е.

$$C_{своевр} = 0{,}1 \cdot (0{,}99 + 0{,}96 + 0{,}80 + 0{,}84 + 0{,}71 + 0{,}73 + 0{,}78 + 0{,}73 + 0{,}69 + 0{,}71) = 0{,}794.$$

Примечание — Значения слагаемых взяты из рисунка Г.7.

Вместе с тем, при расчете интегрального риска в примере 11 используется значение коэффициента своевременности обработки информации, рассчитываемого по формуле (В.13) — именно потому, что все требования к своевременности обработки запросов выполнены, этот коэффициент $Z_{своевр}$ = 1.

Г.7.4 Пример 3 демонстрирует подход к оценке вероятности того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений $P_{полн}$.

Объектами анализа являются информационные сообщения, впервые поступающие в БД, и технологии сбора таких данных от источников в режиме реального времени функционирования СДК.

При проектировании СДК необходимо обосновать варианты построения и функционирования системы сбора информации, обеспечивающей полноту оперативного отражения в системе новых объектов учета и явлений. Требования заказчика сформулированы следующим образом: должна быть обеспечена полнота отражения информации в СДК обо всех реальных событиях и явлениях, в частности, вероятность того, что в СДК полностью отражены состояния всех реально существующих критичных объектов и явлений:

- для чрезвычайных происшествий, угрожающих безопасности людей и среды их обитания, должна быть не ниже 0,98;
- для оперативной информации об обстановке (в т. ч. по условиям функционирования шахты) — не ниже 0,95;
- для статистической информации при управлении СДК — не ниже 0,9;
- для команд и приказов с условиями их выполнения — не ниже 0,95.

Согласно выданным главному конструктору СДК постановкам функциональных задач и принятым неблагоприятным сценариям возникновения и развития возможных аварийных ситуаций установлена ожидаемая частота появления новых объектов учета:

- для информации о чрезвычайных происшествиях — до трех раз в сутки (расчетные варианты i = 1, 2, 3);
- для оперативной информации об обстановке — в среднем до одного раза в час (i = 4, 5, 6);
- для статистической информации при управлении СДК — 2 раза в неделю (i = 7, 8, 9);
- для единожды вводимой информации (команд и приказов с условиями их выполнения) — 6 раз в сутки (i = 10).

Для проведения требуемых оценок технические решения главного конструктора в части сбора информации описаны следующими исходными данными, позволяющими охарактеризовать существенные различия в среднем времени подготовки, передачи и ввода новых объектов учета в БД СДК (именно для анализа этих различий анализируемые варианты снабжены индексом i = 1, …,10).

Для информации о чрезвычайных происшествиях предусмотрена ее подготовка человеком. При этом для детальной информации и ее визуального контроля подготовка занимает в среднем 20 мин (i = 1), для детальной информации с программным контролем — 10 мин (i = 2), для укрупненной информации — до 5 мин (i = 3).

Для оперативной информации об обстановке возможна подготовка ее человеком с визуальным контролем в среднем около 20 мин (i = 4) либо с программным контролем до 10 мин (i = 5), а для некоторых видов информации, формируемой с помощью автоматических датчиков, в среднем за 30 с (i = 6). Т. е. результаты для i = 4 характеризуют существующую систему ручного контроля на местах, а результаты для i = 5, 6 характеризуют СДК.

Для статистической информации возможна подготовка информации человеком в течение 20 мин (i = 7), для детальной информации с программным контролем — до 10 мин (i = 8), для укрупненной информации с программным контролем — до 5 мин (i = 9).

Для команд и приказов информация готовится человеком в среднем в течение 5 мин (i = 10).

Согласно предложенным техническим решениям предусмотрены:

- передача информации от источников по телефону за среднее время до 10 мин (i = 1, 4, 7) или автоматизированно с использованием СДК — до 1 мин (i = 2, 3, 5, 6, 8, 9, 10);
- ввод поступившей информации в БД за среднее время человеком от 1 мин (i = 4) до 10 мин (i = 1, 2, 5, 7, 8) или автоматически в СДК за 20 с (i = 3, 6, 9, 10).

С использованием модели В.3.4 осуществлена количественная оценка полноты оперативного отражения в СДК состояния всех реально существующих критичных объектов и явлений. Результаты расчетов для сравнения описанных вариантов приведены на рисунке Г.8.

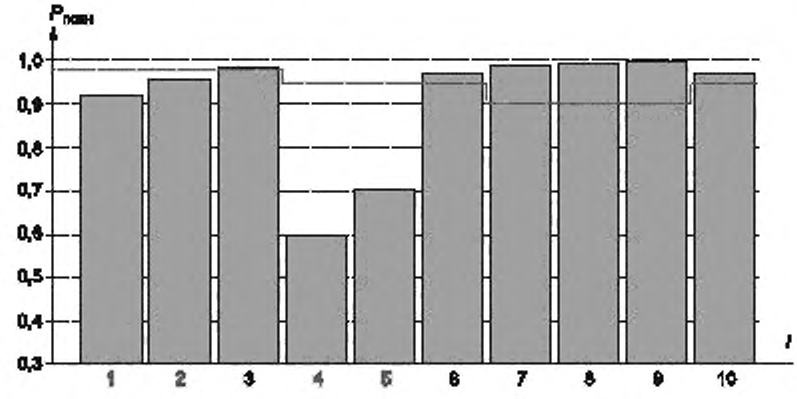


Рисунок Г.8 — Сравнительные оценки вариантов по вероятности того, что в СДК полностью отражены состояния всех реально существующих критичных объектов и явлений

Анализ результатов расчетов показывает (см. рисунок Г.8):

- для информации о новых чрезвычайных происшествиях требованиям заказчика удовлетворяет лишь вариант оперативного обнаружения и подготовки укрупненной информации у источника с программным контролем, передачей через СДК с автоматическим вводом в БД (i = 3);

- для оперативной информации об обстановке требованиям заказчика отвечает лишь вариант с автоматическими датчиками СДК (i = 6). При этом другие варианты обнаружения и подготовки информации в течение 10—20 мин и длительного ввода ее в БД при передаче сколь угодно быстро не позволят обеспечить требуемую полноту оперативного отражения информации;

- для статистической информации при управлении СДК (i = 7, 8, 9) любой способ обнаружения и подготовки информации человеком, передачи любым из выбранных способов обеспечит полноту оперативного отражения в БД информации о реальных объектах учета и явлениях. Это объясняется относительной редкостью появления новой статистической информации;

- требуемая полнота оперативного отражения в системе реальных команд и приказов, поступающих через средства связи СДК (i = 10), будет обеспечена, что гарантируется быстротой передачи.

По результатам системного анализа сделан вывод: из множества сравниваемых технических решений лишь варианты 3, 6 — 10 отвечают задаваемым требованиям. Их реализация позволит обеспечить выполнение изначальных требований заказчика к полноте оперативного отражения в СДК новых объектов учета и явлений. Вместе с тем, заказчик, осознавая привычность работы в условиях неполноты информации на шахте, а также дороговизну технических изменений в проекте, согласился на снижение изначальных требований к полноте оперируемой информации до такого уровня, что предъявляемые условия α (см. В.3.4) по результатам моделирования выполняются. С учетом этого при расчете интегрального риска в примере 11 использован вероятностный коэффициент полноты оперативного отражения в системе новых объектов и явлений $Z_{полн} = 1$.

Нижеследующие примеры 4 — 6 позволяют продемонстрировать подход к оценке достоверности используемой информации в СДК с помощью детальных оценок вероятности сохранения актуальности информации на момент ее использования, определяемой по модели В.3.5, вероятности отсутствия ошибок в информации после ее контроля, определяемой по модели В.3.6 и вероятности получения корректных результатов обработки информации, определяемой по модели В.3.7.

Г.7.5 Пример 4 демонстрирует подход к оценке вероятности сохранения актуальности информации на момент ее использования в системе $P_{акт}$.

Объектами анализа являются информационные ресурсы, обновляющие БД СДК, и технологии синхронизации информационных процессов, обеспечивающих полезность данных СДК в режиме реального времени функционирования шахты.

Важной практической задачей при создании и организации эффективного функционирования СДК является определение научно обоснованного периода обновления данных о состоянии параметров контролируемого оборудования и среды эксплуатации (например, давления, температуры, напряжения, загазованности и др.). С одной стороны, обновление данных по мере значимого изменения состояния оборудования необходимо для обеспечения достоверности информации с последующим ее применением по назначению. С другой стороны, слишком частое обновление этих данных необоснованно перегружает каналы связи и компьютерную память, приводит к программным сбоям, создает недопустимые временные задержки, может рассинхронизировать информационные процессы в СДК, нарушая тем самым режим реального времени функционирования самой СДК и лишая необходимой информационно-аналитической поддержки должностных лиц в процессе управления информацией на шахте. Учитывая результаты примера 3 о достижимости полноты отражения оперативной информации об обстановке с вероятностью не ниже $P_{полн} = 0{,}95$, задача формализована главным конструктором следующим образом: определить такой рациональный период обновления информации в СДК, при котором актуальность используемой информации будет не ниже, чем 0,95.

Анализ совокупности обновляемой информации при круглосуточной загрузке оборудования позволил выявить два варианта условий:

- обычные условия загрузки оборудования, характеризуемые частотой значимого изменения состояния оборудования 36 раз в сутки;

- условия наивысшей загрузки, возникающие для некоторого оборудования случайным образом (например, для вентиляторных установок или МДУ при повышенных скоплениях на местах газа метана), продолжающиеся несколько часов в сутки и характеризуемые частотой значимого изменения состояния оборудования 3 раза в час.

Среднее время съема, передачи и ввода в БД СДК телеметрических данных от оборудования составляет в среднем 16 с. Еще несколько секунд уходит на аналитическую обработку и доведение результатов обработки до пользователей. Это означает, что обновление чаще 25 — 30 с нецелесообразно из-за перегрузки и вычислительной неспособности своевременно обработать такую часто обновляемую информацию от сотен источников.

Моделирование для определения искомого периода обновления информации в СДК осуществлено по этим исходным данным с использованием модели В.3.5. Сравнительные результаты расчетов приведены на рисунках Г.9 — Г.12.

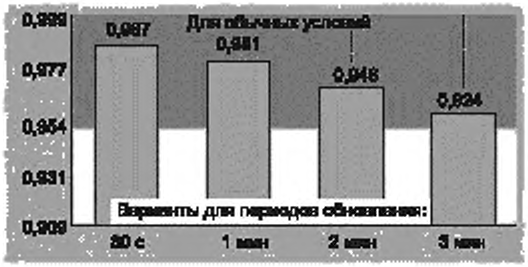


Рисунок Г.9 — Вероятность сохранения актуальности информации для обычных условий загрузки оборудования

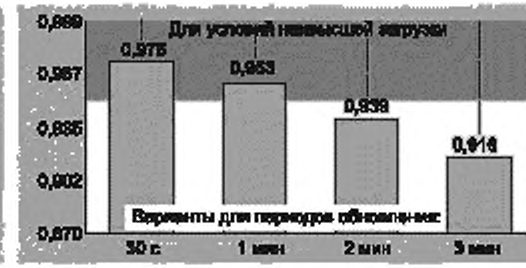


Рисунок Г.10 — Вероятность сохранения актуальности информации для условий наивысшей загрузки оборудования

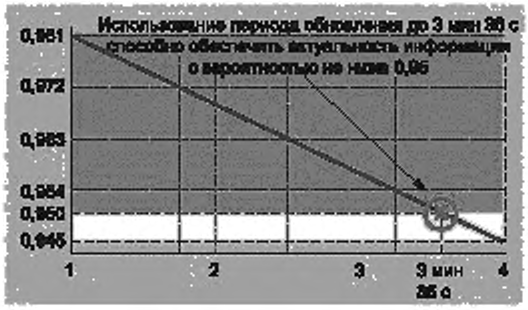


Рисунок Г.11 — Зависимость вероятности сохранения актуальности информации для обычных условий загрузки оборудования от периода обновления (в минутах)

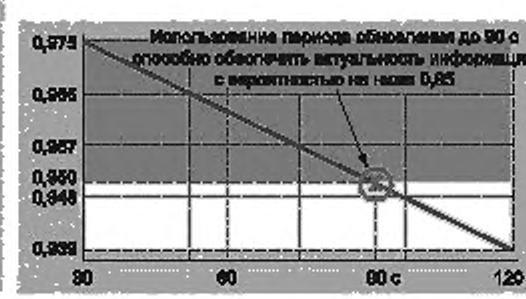


Рисунок Г.12 — Зависимость вероятности сохранения актуальности информации для условий наивысшей загрузки оборудования от периода обновления (в секундах)

Анализ результатов расчетов показывает, что для обеспечения актуальности информации в СДК с вероятностью не ниже 0,95 период обновления может быть выбран следующим образом:

- для обычных условий загрузки оборудования — до 3 мин 36 с;
- для условий наивысшей загрузки — до 90 с.

В результате системного анализа определено: из соображений недопущения вычислительной перегрузки СДК наиболее рациональным в условиях неопределенности функционирования шахты признан период обновления информации в СДК, равный 90 с.

Для определенности при расчете интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации в примере 11 использована достигаемая вероятность сохранения актуальности информации $P_{акт} = 0,95$.

По результатам системного анализа заказчик, осознавая незначительность ущербов и практическую приемлемость работы в условиях не всегда актуальной информации на шахте, согласился с тем, что предъявляемые условия α (см. В.3.5) по результатам моделирования выполняются. С учетом этого при расчете интегрального риска в примере 11 использован вероятностный коэффициент актуальности информации в системе $Z_{акт} = 1$.

Г.7.6 Пример 5 демонстрирует подход к оценке вероятности отсутствия ошибок в информации после ее контроля $P_{безош}$.

Объектами анализа являются информационные ресурсы, вводимые в СДК, и технологии контроля их безошибочности. При проектировании СДК необходимо обосновать технологию контроля информации, обеспечивающую безошибочность входной информации. Требования заказчика сформулированы следующим образом: используемые технологии контроля входной формализованной и неформализованной информации должны обеспечивать ее безошибочность, в частности, вероятность отсутствия ошибки во входном сообщении, вводимом в БД СДК, должна быть не ниже 0,95, при этом допустимое время контроля не должно превышать 10 мин для графических документов и входных обобщенных документов до 10000 знаков и 1 ч для детальных документов объемом до 50000 знаков.

Для проведения требуемых оценок технические решения главного конструктора в части контроля информации описаны следующими исходными данными, позволяющими охарактеризовать существенные различия в рассматриваемых вариантах технологий контроля (именно для анализа этих различий анализируемые варианты снабжены индексом $i = 1,\ldots,10$). Согласно постановкам функциональных задач информация, подлежащая контро-

лю, обладает следующими характеристиками: средний объем коротких документов составляет в среднем 20 контролируемых объектов для графической информации (расчетные варианты i = 1, 2), 10000 текстовых знаков для обобщенных документов (i = 3, 4, 7 — 10) и 50 000 знаков для детальных документов (i = 5, 6).

Для оценки безошибочности информации в СДК технические решения главного конструктора предусматривают осуществление лишь визуального контроля всей информации. С применением настоящей методики осуществляется количественная оценка ожидаемой безошибочности используемой информации и выявление необходимости создания вспомогательных средств программного контроля и обоснования системных требований к ним.

По результатам сравнения с аналогами установлено, что частота ошибок в документах может составлять одну ошибку на 100 графических объектов (i = 1, 2), одну ошибку на 100 знаков (i = 3, 5, 7, 8) или 200 знаков (i = 4, 6) неформализованной информации. В результате натурных экспериментов и сравнения с аналогами установлено, что технология контроля информации характеризуется следующими исходными данными:

- скорость контроля равна 20 объектам в минуту для графической информации (i = 1, 2), 2000 табличным знакам в минуту (i = 3 — 6) без программной поддержки и 6000 знакам в минуту (i = 7 — 10) с использованием средств программного контроля;

- частота ошибок контроля 1-го рода составляет одну ошибку на 100 мин работы для высококвалифицированного контролера (i = 1, 3, 5) и одну ошибку на 50 мин для контролера средней квалификации (i = 2, 4, 6). Кроме того, при поддержке программными средствами контроля частота ошибок 1-го рода может быть снижена на порядок, т. е. для высококвалифицированного контролера она составит одну ошибку на 16 ч (i = 7, 9), а для контролера средней квалификации — одну ошибку на 8 ч (i = 8, 10) работы;

- среднее время наработки на ошибку 2-го рода соответственно составляет 1 ч для высококвалифицированного контролера (i = 1, 3, 5, 7, 9) и 40 мин для среднеквалифицированного (i = 2, 4, 6, 8, 10) контролера;

- среднее непрерывное время работы человека-контролера составляет 45 мин (i = 1—10), после чего следует необходимое восстановление концентрации внимания (вплоть до смены контролера);

- на однократный контроль короткого и обобщенного документа отводится в среднем 10 мин (i = 1—4, 7—10), а на однократный контроль детального документа — 1 ч (i = 5, 6).

При моделировании предусмотрено использование повторного визуального контроля (i = 9, 10), причем в качестве исходной доли ошибок после первого контроля выступают результаты расчетов по настоящей методике соответственно для вариантов i = 7 и i = 8.

С использованием модели В.3.6 по этим исходным данным проведена количественная оценка безошибочности информации после контроля. Сравнительные результаты расчетов приведены на рисунке Г.13 и Г.14.

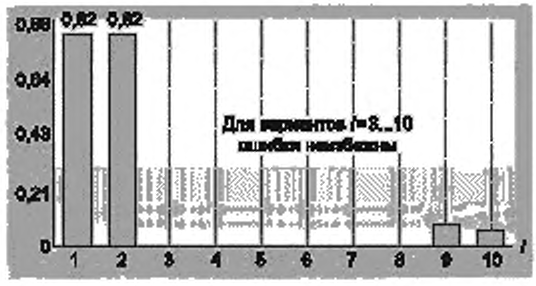


Рисунок Г.13 — Вероятность отсутствия ошибок в информации без контроля для 10 вариантов сравнения

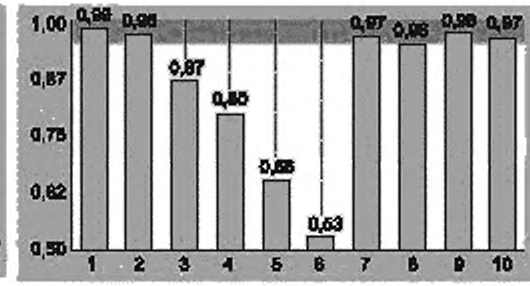


Рисунок Г.14 — Вероятность отсутствия ошибок в информации после контроля для 10 вариантов сравнения

Анализ результатов расчетов показывает:

- для коротких графических документов вероятность отсутствия ошибок после контроля специалистом средней и высокой квалификации превышает 0,98, причем она по-прежнему будет удовлетворять требованиям при возможном увеличении среднего объема контролируемой информации до 40 объектов (i = 1, 2);

- для документов объемом 10 000—50 000 знаков (i = 3—6) ошибки без контроля неизбежны. При контроле без поддержки программными средствами вероятность отсутствия ошибок ниже требуемой (от 0,53 до 0,87) независимо от квалификации проверяющих;

- применение поддерживающих программных средств контроля (i = 7, 8) позволяет повысить вероятность отсутствия ошибок в документах объемом 10 000 знаков до уровня 0,96—0,97;

- применение повторного визуального контроля с использованием программных средств (i = 9, 10) оказывается избыточным как для высококвалифицированных, так и среднеквалифицированных контролеров по сравнению с вариантами i = 7, 8.

Вывод: для выполнения заданных требований выявлена объективная необходимость разработки специальных программных средств поддержки контроля информации в СДК. Рекомендации: основными требованиями к разработке этих программных средств, а в последующем — и для эксплуатационной документации должны быть:

- требования к скорости контроля — не ниже 20 графических объектов в минуту и 6000 текстовых знаков в минуту;
- требования к допустимой частоте ошибок первого рода — не чаще одной ошибки за 500 мин работы;
- требования к допустимой наработке до первого пропуска ошибки — в среднем не менее 40 мин;
- регламентация времени работы человека-контролера, в частности непрерывное время контроля не должно превышать 45 мин.

Учитывая выполнимость сделанных выше вывода и рекомендаций, при расчете интегрального риска в примере 11 использован вероятностный коэффициент безошибочности информации в системе после контроля $Z_{безош} = 1$ (см. В.3.6).

Г.7.7 Пример 6 демонстрирует подход к оценке вероятности получения корректных результатов обработки информации $P_{корр}$.

Объектами анализа являются информационные активы СДК и технологии их обработки по назначению. При проектировании СДК главный конструктор оценивает целесообразность разработки вспомогательных экспертных систем для обработки информации. Заказчик использует настоящую методику для количественной оценки ожидаемой корректности обработки информации в режиме реального времени функционирования СДК, а главный конструктор — для дальнейшего выявления рациональных технических способов удовлетворения требований технического задания. Согласно постановкам функциональных задач ЛПР и операторы (аналитики) анализируют те же объемы информации, что и в примере 5 (см. Г.7.6), но уже с целями подготовки и принятия прагматических решений по обеспечению промышленной безопасности на предприятии. Для проведения требуемых оценок с учетом существенных различий в рассматриваемых вариантах технологий обработки информации анализируемые варианты по-прежнему снабжены индексом $i = 1,\ldots,10$. То есть обобщенная информация характеризуется объемом до 20 объектов ($i = 1, 2$), а детальная информация — объемом до 10 000 знаков ($i = 3, 4, 7—10$) и до 50 000 знаков ($i = 5, 6$). При анализе информации осуществляется не контроль, а семантическая обработка аналитиком. Примером малого объема анализируемой информации может служить обобщенное состояние контролируемых объектов на электронной карте с использованием мнемосхем.

Примером большего объема анализируемой информации может служить детальная информация о контролируемых объектах, например, за комплекс ГВУ, МДУ и иное оборудование шахты. Таковых объектов учета для СДК, охватывающих несколько шахт, могут быть тысячи и десятки тысяч.

Пусть в обобщенной информации малого объема (i = расчетные варианты 1,2) вся информация является принципиальной, в детальной (для $i = 3—10$) процент принципиальной информации не превышает 50 %. В обязанности ЛПР и оператора входят корректные выделение и осмысление этой информации в режиме реального времени для последующего использования ее по назначению. Требуемый уровень корректности обработки информации по выбранному вероятностному показателю — не ниже 0,95.

В результате натурных экспериментов и сравнения с аналогами установлено, что технология обработки информации характеризуется следующими исходными данными. Скорость обработки информации составляет 20 объектов в минуту для ЛПР как высокого ($i = 1, 3, 5, 7, 9$), так и среднего уровня квалификации ($i = 2, 4, 6, 8, 10$) и 2000 знаков в минуту для оператора-аналитика ($i = 3—5$). Использование специальной экспертной системы автоматической обработки данных (целесообразность создания которой оценивается Главным конструктором, $i = 6—10$) позволяет повысить скорость обработки детальной информации аналитиком до 6000 знаков в минуту. Частота ошибок анализа 1-го рода, среднее время наработки на алгоритмическую ошибку и непрерывное время работы человека (ЛПР и оператора) сохраняются теми же, что и в примере 5 для контроля информации. Допустимое время оперативной обработки информации объемом 10 000 знаков составляет 10 мин для $i = 1—4, 7, 8$, при детальной аналитической обработке документов объемом 50 000 знаков — до одного часа ($i = 5, 6$).

Моделирование осуществлено по этим исходным данным с использованием рекомендаций В.3.7.

Анализ обобщенных результатов расчетов, приведенных на рисунках Г.15 и Г.16, показывает:

- вероятность получения корректных результатов обработки обобщенной информации составляет 0,96 — 0,97 для ЛПР как среднего, так и высокого уровня квалификации ($i = 1, 2$) из-за сравнительно небольшого объема анализируемой информации. Часть неучтенной информации не превысит 5 %;
- для документов объемом 10000 знаков за счет применения специальной экспертной системы ($i = 7, 8$) корректность обработки информации оператором как среднего, так и высокого уровня квалификации составит 0,96—0,97 ($i = 7, 8$) против 0,80 — 0,88 (для $i = 3, 4$), характерных для варианта обработки информации без ее использования. При этом часть неучтенной информации составит для $i = 7, 8$ лишь 1.5 % — 2.2 % против 6.2 % — 10.1 % для $i = 3, 4$;
- для документов объемом 50000 знаков применение оператором экспертной системы ($i = 6$) позволит повысить вероятность корректной обработки до уровня 0,81 против 0,66 без ее использования ($i = 5$), но для корректности обработки информации этого явно недостаточно;
- использование в автоматическом режиме специальной экспертной системы обеспечит корректность обработки лишь на уровне 0.58—0,59 ($i = 9, 10$), что объясняется слабой производительностью применяемых программно-технических средств, не позволяющих за одну минуту автоматически обработать весь объем принципиальной информации. Часть неучтенной информации превысит 20 %.

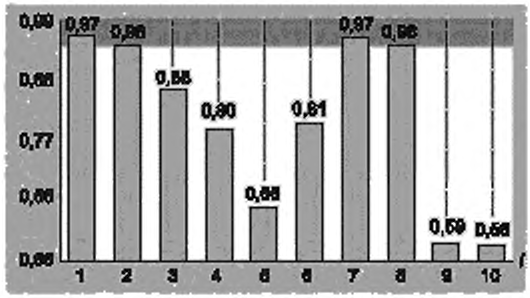


Рисунок Г.15 — Вероятность получения корректных результатов обработки информации для 10 вариантов сравнения

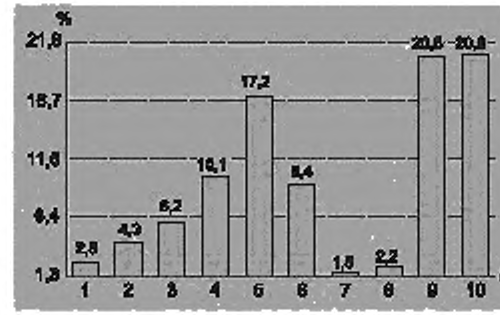


Рисунок Г.16 — Часть принципиальной информации, не учтенная в процессе обработки для 10 вариантов сравнения

Учитывая потенциальные возможности специальной экспертной системы поддержки принятия решений и ее осуществимость, при расчете интегрального риска в примере 11 использован вероятностный коэффициент корректности обработки информации в системе $Z_{корр} = 1$ (см. В.3.7).

Г.7.8 Пример 7 демонстрирует подход к оценке вероятности безошибочных действий пользователей и персонала в течение заданного периода прогноза $P_{чел}(T_{зад})$.

Объектами анализа являются мастера шахты, осуществляющие мониторинг функционирования комплекса ГВУ, комплекса МДУ и газоотсасывающей установки, охваченных функциональными возможностями СДК. Структура моделируемой системы представлена на рисунке Г.17, она полностью аналогична структуре, представленной на рисунке Г.3. Отличие лишь в том, что элементами моделируемой системы являются мастера, а резервирование означает, что для ГВУ 1, ГВУ 2, МДУ 1, МДУ 2 мониторинг осуществляют 2 мастера, взаимно контролирующие друг друга. Возможные ущербы при ошибках пользователей и персонала и логическая интерпретация состояний моделируемой системы полностью аналогичны тем, что изложены в примере 1.

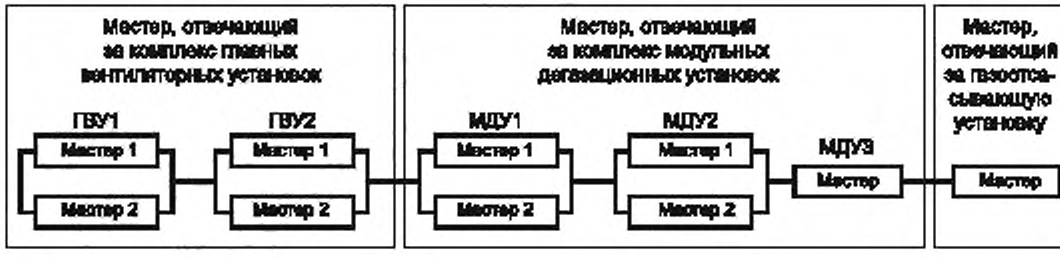


Рисунок Г.17 — Моделируемая система для оценки безошибочных действий мастеров

Исходные данные для оценки вероятности безошибочных действий мастеров представлены в таблице Г.2. Остальные исходные данные — те же, что и в таблице Г.1, с теми же комментариями:

- среднее время развития угроз с момента возникновения источников угроз до нарушения $\beta = 30$ мин;
- среднее время диагностики $T_{диаг} = 1$ мин;
- среднее время восстановления после выявления нарушений $T_{восст} = 20$ мин;
- задаваемая длительность периода прогноза $T_{зад} = 1$ мес.

Моделирование осуществлено по этим исходным данным с использованием рекомендаций В.3.8.

Системный анализ результатов расчетов показывает, что вероятность безошибочных действий пользователей и персонала будет выше 0,96 (см. рисунок Г.18). По показателю безошибочности действия всех мастеров в моделируемых условиях приблизительно равнопрочны.

В свою очередь анализ зависимости вероятности безошибочных действий мастеров от периода прогноза (см. рисунок Г.19) позволил установить: в условиях примера безошибочные действия всех мастеров будут обеспечены в течение периода до 42 дней с вероятностью не ниже 0,95.

Таблица Г.2 — Исходные данные для оценки вероятности безошибочных действий мастеров

Исходные данные	Значения и комментарии					
	Комплекс главных вентиляторных установок		Комплекс модульных дегазационных установок			Газоотсасывающая установка
	ГВУ 1 (для каждого вентилятора)	ГВУ 2 (для каждого вентилятора)	МДУ 1 (для каждого насоса)	МДУ 2 (для каждого насоса)	МДУ 3	
σ — частота возникновения источников угроз	1 раз в год (соизмеримо с возникновением предпосылок к ошибкам, свойственным мастеру средней квалификации)		1 раз в 5 лет (соизмеримо с возникновением предпосылок к ошибкам, свойственным мастерам высокой квалификации)			
$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики	10 минут (мониторинг осуществляют два мастера, взаимно контролирующие друг друга)					1 час (мониторинг осуществляет один мастер, контроль — со стороны начальника)

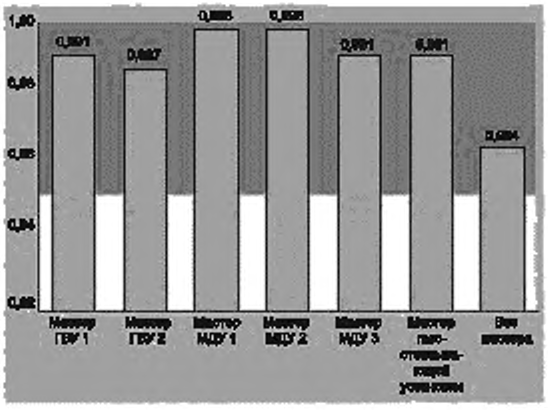


Рисунок Г.18 — Оценки вероятности безошибочных действий мастеров в течение месяца

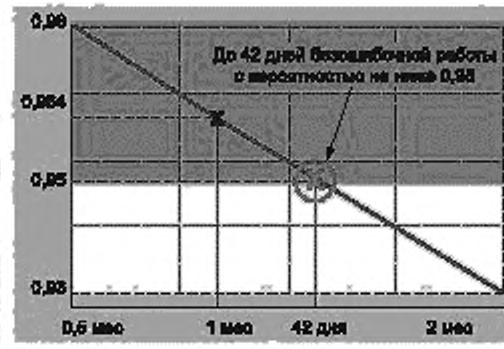


Рисунок Г.19 — Зависимость вероятности безошибочных действий всех мастеров от периода прогноза длительностью от 0,5 месяца до 2 месяцев

Ориентируясь на приемлемый уровень вероятности безошибочных действий мастеров за месяц не ниже 0,95, при расчете интегрального риска в примере 11 использован коэффициент безошибочных действий пользователей и персонала системы в течение месяца $Z_{чел}(T_{зад}) = 1$ (см. В.3.8).

Нижеследующие примеры 8—10 (см. Г.7.9 — Г.7.11) позволяют продемонстрировать подход к оценке вероятности приемлемого выполнения требований по защите информации в течение заданного периода прогноза с помощью детальных оценок вероятности отсутствия опасного программно-технического воздействия на СДК по модели В.3.9.2, вероятности обеспечения защищенности активов шахты от НСД по модели В.3.9.3, вероятности сохранения конфиденциальности используемой информации по модели В.3.9.4.

Г.7.9 Пример 8 демонстрирует подход к оценке вероятности отсутствия опасного программно-технического воздействия на СДК в течение заданного периода прогноза $P_{возд}(T_{зад})$.

Объектами анализа являются программное обеспечение и информационные массивы СДК, используемые при мониторинге функционирования комплекса ГВУ, комплекса МДУ и газоотсасывающей установки. Структура моделируемой системы для оценки защищенности СДК от опасного программно-технического воздействия представлена на рисунке Г.20. Она логически связана со структурами, представленными на рисунках Г.3 и Г.17, однако все аспекты резервирования рассматриваются на уровне элементов, представимых как «черные ящики».



Рисунок Г.20 — Моделируемая система для оценки защищенности СДК от опасного программно-технического воздействия

Исходные данные для оценки вероятности отсутствия опасного программно-технического воздействия на СДК представлены в таблице Г.3. Согласно модели угроз безопасности информации, принятой руководством шахты, для СДК моделируемый сценарий предполагает маскировку опасных программно-технических воздействий под обычные отказы оборудования. С учетом предполагаемой маскировки частота возникновения источников угроз (например, внедрения программных закладок или заражение неизвестным компьютерным вирусом) сохранена в настоящем примере такой же, как и для примера 1.

Остальные исходные данные аналогичны данным из таблицы Г.1:

- среднее время между окончанием предыдущей и началом очередной диагностики =5 мин с учетом переключения внимания диспетчера на выполнение разных функций;
- среднее время диагностики $T_{диаг}$ = 1 мин, включая необходимую отдачу распоряжений;
- среднее время восстановления после выявления нарушений $T_{восст}$ = 20 мин (это среднее время переинсталляции программного обеспечения и восстановления информационных массивов);
- задаваемая длительность периода прогноза $T_{зад}$ = 1 мес.

Моделирование осуществлено по этим исходным данным с использованием рекомендаций В.3.9.2.

Системный анализ результатов расчетов показал, что при ориентации на противодействие составных элементов моделируемой системы опасным компьютерным воздействиям оцениваемая вероятность отсутствия опасного программно-технического воздействия на каждый из активов в течение месяца будет не ниже 0,998 (см. рисунок Г.21). По этому показателю все активы СДК в моделируемых условиях приблизительно равнопрочны.

Таблица Г.3 — Исходные данные для оценки вероятности отсутствия опасного программно-технического воздействия на СДК в течение заданного периода прогноза

Исходные данные	Значения и комментарии					
	Программное обеспечение и информационные массивы СДК, используемые при мониторинге функционирования шахты					
	Комплекс ГВУ		Комплекс МДУ			Активы газоотсасывающей установки
	Активы ГВУ 1	Активы ГВУ 2	Активы МДУ 1	Активы МДУ 2	Активы МДУ 3	
σ — частота возникновения источников угроз	1 раз в месяц	1 раз в 2 месяца (т. е. в 2 раза выше по сравнению с угрозами для активов ГВУ 1)	1 раз в 3 месяца (т. е. в 3 раза выше по сравнению с угрозами для активов ГВУ 1)	1 раз в 6 месяцев (т. е. в 2 раза выше по сравнению с угрозами для активов МДУ 1)	1 раз в год (т. е. в 4 раза выше по сравнению с угрозами для активов МДУ 1)	1 раз в 2 года (т. е. в 24 раза выше по сравнению с угрозами для активов ГВУ 1 и в 8 раз выше по сравнению с МДУ 1)
β — среднее время развития угроз с момента возникновения источников угроз до нарушения	1 сутки (предполагается, что из-за маскировки источники угроз активизируются не сразу, а с некоторой задержкой, не менее суток)					

В свою очередь, анализ зависимости вероятности отсутствия опасного программно-технического воздействия от периода прогноза (см. рисунок Г.22) позволил установить: в условиях примера защищенность программного обеспечения и информационных массивов СДК будет обеспечена в течение периода до 2 мес с вероятностью не ниже 0,992.

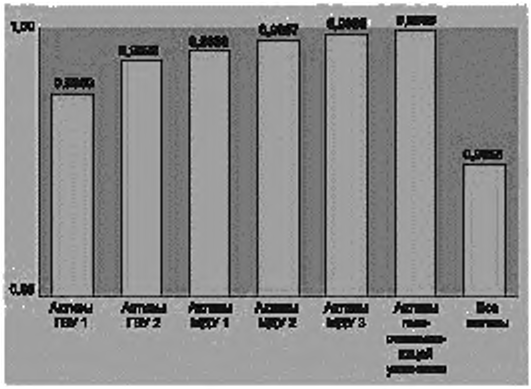


Рисунок Г.21 — Оценки вероятности отсутствия опасного программно-технического воздействия в течение месяца

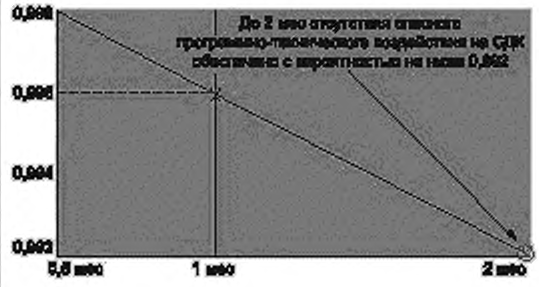


Рисунок Г.22 — Зависимость вероятности отсутствия опасного программно-технического воздействия на все активы от периода прогноза длительностью от 0,5 месяца до 2 месяцев

Для определенности при расчете интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации в примере 11 использована достигаемая вероятность отсутствия опасного программно-технического воздействия на СДК в течение месяца $P_{возд}(T_{зад}) = 0,996$.

Г.7.10 Пример 9 демонстрирует подход к оценке вероятности обеспечения защищенности активов СДК от несанкционированного доступа $P_{НСД}$.

Объектами анализа являются информационные и программные ресурсы СДК для построения на шахте эффективной защиты от НСД.

Защита от НСД строится на практике как последовательность преград, после успешного преодоления которых злоумышленник получает доступ к информационным и/или программным ресурсам СДК. Анализируются возможности и целесообразность создания 10 преград для защиты от НСД. На основании модели угроз в таблице Г.4 отражены предполагаемые характеристики сценария угроз НСД и системы защиты информации.

Моделирование осуществлено по этим исходным данным с использованием рекомендаций В.3.9.3. Результаты расчетов отражены на рисунке Г.23.

Таблица Г.4 — Характеристики сценария угроз НСД и системы защиты

Преграда	Частота смены значения параметра преграды	Среднее время преодоления преграды нарушителем	Возможный способ преодоления преграды
1. Охраняемая территория со сменой охраны	через 2 ч	30 мин	Скрытое проникновение на территорию
2. Пропускная система на объект СДК (в т. ч. доступ к рабочим местам пользователей со сменой службы контроля)	через 1 сут	10 мин	Подделка документов, сговор, обман
3. Электронный ключ для включения компьютера	через 5 лет (наработка до замены)	1 нед	Кража, принудительное изымание ключа, сговор
4. Пароль для входа в систему	через 1 мес	1 мес	Подсматривание, принудительное выпытывание, сговор, подбор пароля
5. Пароль для доступа к программным устройствам	через 1 мес	10 сут	Подсматривание, принудительное выпытывание, сговор, подбор пароля
6. Пароль для доступа к требуемой информации	через 1 мес	10 сут	Подсматривание, принудительное выпытывание, сговор, подбор пароля
7. Зарегистрированный внешний носитель информации для записи	через 1 год	1 сут	Кража, принудительная регистрация, сговор

Окончание таблицы Г.4

Преграда	Частота смены значения параметра преграды	Среднее время преодоления преграды нарушителем	Возможный способ преодоления преграды
8. Подтверждение подлинности пользователя в процессе сеанса	через 1 мес	1 сут	Подсматривание, принудительное выпытывание, сговор
9. Телемониторинг	через 5 лет (наработка до замены)	2 сут	Имитация неисправности, ложные ролики, маскировка под персонал, сговор
10. Шифрование информации со сменой ключей	через 1 мес	2 года	Расшифровка, сговор

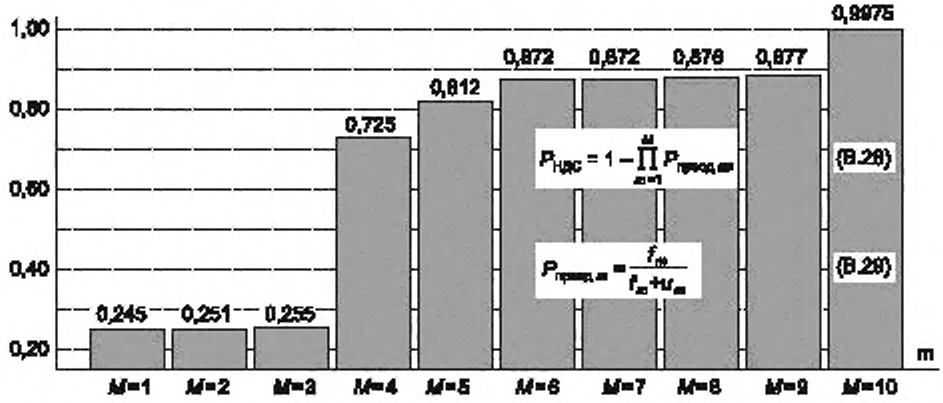


Рисунок Г.23 — Рост вероятности обеспечения защищенности активов СДК от НСД с увеличением количества и качества преград, $m = 1,\ldots,M$

Анализ полученных результатов расчета показывает следующее.

Первые 3 преграды преодолеваются с вероятностью около 0,745. Использование сменяемых паролей один раз в месяц для 4, 5 и 6 преград позволяет в три раза поднять защищенность с 0,255 до 0,872. Однако, общая защищенность системы после введения первых шести преград остается слабой (0,872).

Введение 7, 8, 9 преград практически бесполезно, т.к. не обеспечивает заметного повышения защищенности системы для заданных значений исходных данных (0,877 по сравнению с 0,872).

Использование криптографических средств защиты (10-я преграда) позволяет более существенно повысить защищенность информационных ресурсов от НСД — до уровня 0,9975.

Примечание — Модель В.3.9.4 при прочих равных условиях позволяет в сравнении с примененной моделью В.3.9.3 дополнительно учесть длительность периода объективной конфиденциальности информации, который может быть рассмотрен как задаваемый период прогноза (см. пример 10 в Г.7.11).

Для определенности при расчете интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации в примере 11 использована достигаемая вероятность обеспечения защищенности активов СДК от НСД $P_{НСД} = 0{,}9975$.

Г.7.11 Пример 10 демонстрирует подход к оценке вероятности сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $P_{конф}(T_{конф})$.

Объектами анализа являются те же информационные и программные ресурсы СДК при тех же используемых преград системы защиты от НСД. Дополнительно учтена длительность периода объективной конфиденциальности информации. С учетом того, что большинство примеров ориентированы на период прогноза 1 мес, в примере роль периода объективной конфиденциальности информации играет именно этот период прогноза (см. примечание к модели В.3.9.4). Характеристики десяти преград те же, что и в примере 9 (см. таблицу Г.4).

Моделирование осуществлено по исходным данным таблицы Г.4 с заданием $T_{конф}$ = 1 мес и использованием рекомендаций В.3.9.4. Результаты расчетов отражены на рисунке Г.24.

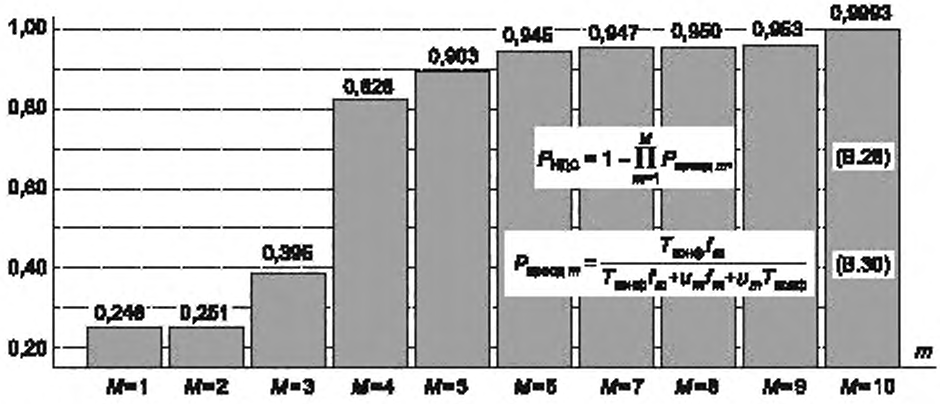


Рисунок Г.24 — Рост вероятности сохранения конфиденциальности используемой информации с увеличением количества и качества преград, $m = 1,\ldots,M$

Системный анализ полученных результатов расчета показывает следующее.

Использование первых 6 преград (охрана, пропускной режим, электронный ключ и различные системы паролей) обеспечит конфиденциальность информации с вероятностью не выше 0,945.

Использование всех 10 преград обеспечит требуемую конфиденциальность информации в системе: 0,9993, что более, чем в 1400 раз превышает вероятностный риск нарушения конфиденциальности информации [0,9993/(1 — 0,9993)]. В условиях примера это может рассматриваться как обоснованное значение показателя эффективности защиты информации.

Для определенности при расчете интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации в примере 11 использована достигаемая вероятность сохранения конфиденциальности используемой информации в течение месяца $P_{конф}(T_{конф}) = 0,9993$.

Г.7.12 Пример 11 демонстрирует подход к прогнозированию интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации $R_{интегр}(T_{зад})$.

Используя результаты примеров 1 — 10 (см. Г.1.2 — Г.7.11) и модель В.3.10, по формулам (В.31) — (В.33) получаются следующие окончательные результаты примеров для периода прогноза $T_{зад} = 1$ мес:

- по формуле (В.32) вероятность нарушения надежности реализации процесса управления информацией системы в течение периода прогноза без учета требований по защите информации

$$R_{надежн}(T_{зад}) = 1 - Z_{над\ предст}(T_{зад}) \cdot Z_{своевр} \cdot Z_{полн} \cdot Z_{акт} \cdot Z_{безош} \cdot Z_{корр} \cdot Z_{чел}(T_{зад}) = 1 - 0,786 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 0,214;$$

- по формуле (В.33) вероятность нарушения требований по защите информации в системе для процесса управления информацией в течение периода прогноза (с детализацией защищенности от опасных программно-технических воздействий, от НСД, сохранения конфиденциальности информации)

$$R_{наруш}(T_{зад}) = 1 - P_{возд}(T_{зад}) \cdot P_{НСД}(T_{зад}) \cdot P_{конф}(T_{конф}) = 1 - 0,996 \cdot 0,9975 \cdot 0,9993 = 0,0072;$$

- по формуле (В.31) с учетом возможного ущерба интегральный риск нарушения реализации процесса управления информацией системы с учетом требований по защите информации

$$R_{интегр}(T_{зад}) = 1 - [1 - 0,214][1 - 0,0072] \approx 0,220.$$

Вывод: уровень риска нарушения требований по защите информации в процессе управления информацией системы в течение одного месяца (0,0072) в 30 раз меньше по сравнению с интегральным риском (0,220). Качество используемой информации в СДК на приемлемом уровне. Главное узкое место — неудовлетворительная надежность оборудования шахты, выявленная при системном анализе надежности предоставления информации в СДК.

Тем самым в рамках примеров продемонстрированы способы достижения целей прогнозирования рисков с использованием настоящих методических указаний.

Примечание — Другие примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Г.8 Материально-техническое обеспечение

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

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

Г.9 Отчетность

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

Приложение Д
(справочное)

Типовые допустимые значения для расчетных показателей

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

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

Требования системной инженерии при допустимых рисках, свойственных конкретной системе или ее аналогу и 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 надежности реализации процесса управления информацией системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Типовые допустимые значения показателей рисков для процесса управления информацией системы отражены в таблице Д.1. Типовые допустимые значения показателей, характеризующих надежность и своевременность предоставления, полноту, достоверность и безопасность используемой информации в процессе управления информацией системы отражены в таблице Д.2. При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые, а для вероятностей успешного развития событий были не ниже допустимых. В этом случае для задаваемых при моделировании условий имеет место гарантия качества и безопасности реализации процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Пример задания допустимых значений рисков

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

Таблица Д.2 — Пример задания допустимых значения показателей, характеризующих надежность и своевременность предоставления, полноту, достоверность и безопасность используемой информации

Показатель	Допустимое значение для обеспечения качества информации	
	при допустимом риске заказчика	при риске заказчика, соизмеримом с обоснованием для системы-эталона
Вероятность надежного предоставления информации в системе (модель В.3.2)	Не ниже 0,95	Не ниже 0,99
Вероятность своевременной обработки запросов в системе (модель В.3.3)	Не ниже 0,70	Не ниже 0,90
Относительная доля своевременно обработанных в системе запросов (модель В.3.3)	Не ниже 0,90	Не ниже 0,95
Вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений (модель В.3.4)	Не ниже 0,70	Не ниже 0,90
Вероятность сохранения актуальности информации в системе на момент ее использования (модель В.3.5)	Не ниже 0,80	Не ниже 0,90
Вероятность отсутствия ошибок в информации после ее контроля (модель В.3.6)	Не ниже 0,95	Не ниже 0,97
Вероятность получения корректных результатов обработки информации (модель В.3.7)	Не ниже 0,90	Не ниже 0,95
Вероятность обеспечения безошибочных действий пользователей и персонала системы (модель В.3.8)	Не ниже 0,90	Не ниже 0,95
Вероятность отсутствия опасного программно-технического воздействия на систему (модель В.3.9.2)	Не ниже 0,90	Не ниже 0,95
Вероятность обеспечения защищенности активов системы от НСД (модель В.3.9.3)	Не ниже 0,95	Не ниже 0,99
Вероятность сохранения конфиденциальности информации (модель В.3.9.4)	Не ниже 0,995	Не ниже 0,999

Приложение Е
(справочное)

Примерный перечень методик системного анализа для процесса управления информацией системы

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

Е.2 Комплекс методик расчета вероятностных показателей, характеризующих надежность и своевременность предоставления, полноту, достоверность и безопасность используемой информации.

Е.3 Методика количественного обоснования требований к системе и необходимых условий для обеспечения надежности предоставления информации.

Е.4 Методика количественного обоснования требований к системе и необходимых условий для обеспечения своевременности предоставления информации.

Е.5 Методика количественного обоснования требований к системе и необходимых условий для обеспечения полноты отражения состояния всех реально существующих критичных объектов и явлений.

Е.6 Методика количественного обоснования требований к системе и необходимых условий для обеспечения актуальности информации на момент ее использования.

Е.7 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности информации после ее контроля.

Е.8 Методика количественного обоснования требований к системе и необходимых условий для получения корректных результатов обработки информации.

Е.9 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности действий пользователей и персонала.

Е.10 Методика количественного обоснования требований к системе и необходимых условий для обеспечения отсутствия опасного программно-технического воздействия на систему в пределах допустимого риска.

Е.11 Методика количественного обоснования требований к системе для обеспечения защищенности активов системы от НСД в пределах допустимого риска.

Е.12 Методика количественного обоснования требований к системе для сохранения конфиденциальности информации в пределах допустимого риска.

Е.13 Методика прогнозирования интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации.

Е.14 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации).

Е.15 Методики выявления явных и скрытых недостатков процесса управления информацией системы с использованием прогнозирования рисков.

Е.16 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления информацией системы и противодействие угрозам нарушения требований по защите информации (с использованием прогнозируемых рисков).

Е.17 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления информацией системы (с использованием прогнозируемых рисков).

Примечания

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

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

Библиография

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ключевые слова: актив, защита информации, качество информации, процесс управления информацией системы, модель, риск, система, системная инженерия

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 19.05.2021. Подписано в печать 09.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 6,32.

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