ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 59332— 2021**

## Системная инженерия

# ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ПОРТФЕЛЕМ ПРОЕКТОВ

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), Обществом с ограниченной ответственностью «Научно-исследовательский институт прикладной математики и сертификации» (ООО НИИПМС)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 апреля 2021 г. № 308-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 портфелем проектов . . . . . 8
5 Общие требования системной инженерии по защите информации в процессе управления портфелем проектов . . . . . 10
6 Специальные требования к количественным показателям . . . . . 11
7 Требования к системному анализу . . . . . 14
Приложение А (справочное) Пример перечня защищаемых активов . . . . . 15
Приложение Б (справочное) Пример перечня угроз . . . . . 16
Приложение В (справочное) Типовые модели и методы прогнозирования рисков . . . . . 17
Приложение Г (справочное) Типовые допустимые значения показателей рисков для процесса управления портфелем проектов . . . . . 23
Приложение Д (справочное) Примерный перечень методик системного анализа для процесса управления портфелем проектов . . . . . 24
Библиография . . . . . 25

## 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, человеческими ресурсами, качеством, знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335. Для процесса управления портфелем проектов — по настоящему стандарту;
- для процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343;
- для технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы — по ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357.

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

Для планируемого и реализуемого процесса управления портфелем проектов применение настоящего стандарта обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Системная инженерия**

# ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ПОРТФЕЛЕМ ПРОЕКТОВ

System engineering. Protection of information in project portfolio management process

**Дата введения —2021—11—30**

## 1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа для процесса управления портфелем проектов применительно к вопросам защиты информации и специальные требования к используемым количественным показателям.

Для практического применения в приложениях А—Д приведены примеры перечней активов, подлежащих защите, и угроз безопасности информации, типовые модели и методы прогнозирования рисков, типовые допустимые значения для показателей рисков, примерный перечень методик системного анализа.

Примечание — Оценка ущербов выходит за рамки настоящего стандарта. Для разработки самостоятельной методики по оценке ущербов учитывают специфику проектов и 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) и эксплуатации различных систем и реализующими процесс управления портфелем проектов, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации (см. примеры систем в [1]—[24]).

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

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

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ 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 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 9000 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

ГОСТ Р ИСО/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 20000-1 Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами

ГОСТ Р ИСО 21500 Руководство по проектному менеджменту

ГОСТ Р ИСО 21504 Управление проектами, программами и портфелем проектов. Руководство по управлению портфелем проектов

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.5 (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 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 54869 Проектный менеджмент. Требования к управлению проектом

ГОСТ Р 56715.2 Проектный менеджмент. Системы проектного менеджмента. Часть 2. Процессы и процессная модель

ГОСТ Р 56716 Проектный менеджмент. Техника сетевого планирования. Общие положения и терминология

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

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

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

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

ГОСТ Р 57363 Управление проектом в строительстве. Деятельность управляющего проектом (технического заказчика)

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

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 59345—2021 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—2021 Системная инженерия. Защита информации в процессе определения архитектуры системы

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

## 3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 34.003, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 59329, ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1.1

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

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

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

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.3

**заинтересованные стороны в проекте:** Лица или организации, чьи интересы могут быть затронуты в ходе реализации проекта.

[ГОСТ Р 54869—2011, пункт 3.5]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.5

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.6

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.7

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

[ГОСТ Р 50922—2006, статья 2.3.4]

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

3.1.9 **надежность реализации процесса управления портфелем проектов:** Свойство процесса управления портфелем проектов сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса в заданных условиях его реализации в приемлемые сроки.

3.1.10

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.11

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.12

**портфель проектов:** Набор компонентов, которые группируются вместе с целью эффективного управления и для достижения стратегических целей организации.

[ГОСТ Р 54870—2011, пункт 3.8]

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

3.1.14

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

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

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

[ГОСТ Р 57193—2016, пункт 4.1.43]

3.1.15

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

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

[ГОСТ Р 57193—2016, пункт 4.1.1]

3.1.16

**проект:** Комплекс взаимосвязанных мероприятий, направленный на создание уникального продукта или услуги в условиях временных и ресурсных ограничений.

[ГОСТ Р 54870—2011, пункт 3.12]

3.1.17

**риск:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.18

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

Примечания

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

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

[ГОСТ Р 57193—2016, пункт 4.1.44]

3.1.19

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.1.20

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

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

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

3.1.21

**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]

3.1.22 **целостность портфеля проектов:** Состояние портфеля проектов, которое в течение задаваемого периода прогноза отвечает целевому назначению каждого из проектов, входящих портфель.

3.1.23

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использовано сокращение:

ТЗ — техническое задание.

## 4 Основные положения системной инженерии по защите информации в процессе управления портфелем проектов

### 4.1 Общие положения

Организация использует процесс управления портфелем проектов для достижения своих стратегических целей путем оптимизации мониторинга и контроля, управления изменениями портфеля проектов в условиях ограничений и неопределенностей. Управление портфелем проектов обеспечивает связь между уровнем стратегического управления в организации и уровнем управления проектами. Управление портфелем проектов включает в себя комплекс взаимосвязанных организационных методов и действий, с использованием которых организация выделяет и распределяет ресурсы, необходимые для достижения стратегических целей проекта.

В процессе управления портфелем проектов осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса.

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

Определение выходных результатов процесса управления портфелем проектов и типовых действий по защите информации осуществляют по ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 21500, ГОСТ Р ИСО 21504, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р 54869, ГОСТ Р 56715.2, ГОСТ Р 56716, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Оценку интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59349, ГОСТ Р 59355. При этом учитывают специфику организации, применяющей процесс, и проектов, входящих в портфель, — см., например, [21]—[24].

### 4.2 Цели процесса и назначение мер защиты информации

4.2.1 Определение целей процесса управления портфелем проектов осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО 21504, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 53647.1, ГОСТ Р 54869, ГОСТ Р 56715.2, ГОСТ Р 56716, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики организации, применяющей процесс, и самих проектов, входящих портфель проектов.

В общем случае главной целью процесса управления портфелем проектов являются инициация и поддержание необходимых проектов, направленных на достижение стратегических целей организации. В рамках этого процесса для выбранных и согласованных проектов осуществляется адекватное финансирование и выполняется обеспечение ресурсами, санкционируются необходимые полномочия. Обеспечивается постоянный контроль за тем, чтобы проекты были обоснованы и непрерывно инвестировались, в противном случае они перенаправляются для проведения требуемого обоснования и обеспечения соответствующих инвестиций.

Управление портфелем проектов связано с необходимостью последовательного подхода к управлению стратегически согласованными проектами, программами, портфелями и другими связанными мероприятиями, проводимыми в организационной среде, с различной сложностью и неопределенностью. При этом управление должно быть направлено на то, чтобы обеспечивать необходимые инвестиции для портфеля проектов, оптимизировать производственные возможности организации, максимизировать эффекты от инвестиций, определяя потребности и требования заинтересованных сторон.

4.2.2 Меры защиты информации в процессе управления портфелем проектов 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 51275, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59346, ГОСТ Р МЭК 61508-7, [19]—[24] с учетом специфики организации, применяющей процесс, а также проектов, входящих в портфель проектов.

### 4.3 Стадии и этапы жизненного цикла

Процесс управления портфелем проектов относится к категории процессов организационного обеспечения проектов, поэтому задействован на всех стадиях и этапах жизненного цикла систем, создаваемых (модернизируемых, развиваемых) и эксплуатируемых организацией и связанных с проектами, входящими в портфель проектов. Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации систем, связанных с проектами, устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования систем, входящих в портфель проектов. Перечень этапов и конкретных работ в жизненном цикле систем формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 20000-1, 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 портфелем проектов может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

### 4.4 Основные принципы

При проведении системного анализа процесса управления портфелем проектов руководствуются основными принципами, определенными в ГОСТ Р 59349, с учетом дифференциации требований по защите информации в зависимости от категории значимости проектов, входящих портфель, и важности информации, предполагаемой к обработке в рамках систем, связанных с этими проектами, — 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 портфелем проектов сосредотачивают:

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

## 5 Общие требования системной инженерии по защите информации в процессе управления портфелем проектов

5.1 Требования системной инженерии по защите информации устанавливают в соответствии с нормативами, положениями, политиками и процедурами, принятыми в организации, выполняющей этот процесс, с учетом нормативно-правовых документов Российской Федерации (см., например [1]—[24]), уязвимостей самого процесса, преднамеренных и непреднамеренных угроз нарушения его реализации и безопасности информации, а также задействованных при его реализации программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

Поскольку элементы процесса управления портфелем проектов 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 к защите информации призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации процесса управления портфелем проектов и по поддержке при этом эффективности защиты информации.

Требования системной инженерии к защите информации в процессе управления портфелем проектов включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессе управления портфелем проектов определяют по ГОСТ 2.114, ГОСТ 7.32, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 21500, ГОСТ Р ИСО 21504, ГОСТ Р 51583, ГОСТ Р 53647.1, ГОСТ Р 54869, ГОСТ Р 56715.2, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57363, ГОСТ Р 57839 с учетом специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем, и/или систем, выводимых из эксплуатации и связанных с соответствующими проектами (входящими в портфель проектов).

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

5.5 Определение активов, информация которых или о которых подлежит защите, формирование перечня потенциальных угроз надежности реализации процесса и безопасности информации и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 21500, ГОСТ Р ИСО 21504, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 53647.1, ГОСТ Р 54869, ГОСТ Р 56715.2, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57363, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 20000-1, 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 МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-6, [19]—[24].

Примеры перечней учитываемых активов и угроз в процессе управления портфелем проектов приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процесса управления портфелем проектов анализируют по показателям рисков в зависимости от специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем и/или систем, выводимых из эксплуатации и связанных с проектами (входящими в портфель проектов), целями их применения и возможными угрозами. В системном анализе процесса используют модель угроз безопасности информации.

Системный анализ процесса осуществляют с использованием моделей, методов и методик (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13381-1, ГОСТ

Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 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, [19]—[24].

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

Типовые модели и методы прогнозирования рисков процесса управления портфелем проектов, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д. Характеристики мер защиты информации и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемой и накапливаемой статистики по рассматриваемым процессам и возможным условиям их реализации.

## 6 Специальные требования к количественным показателям

### 6.1 Общие положения

6.1.1 В приложении к защищаемым активам, действиям и выходным результатам процесса управления портфелем проектов, к которым предъявлены определенные требования по защите информации, выполняют оценку эффективности защиты информации на основе прогнозирования рисков. Для обоснования эффективных предупреждающих действий по снижению риска или его удержанию в допустимых пределах используют системный анализ.

6.1.2 В общем случае основными выходными результатами процесса управления портфелем проектов являются:

- информация, влияющая на стратегические решения в управлении организацией и портфелем проектов (рыночная конъюнктура, требования законодательства, изменения политической обстановки и др.);
- стратегические цели и приоритеты организации в части управления портфелем проектов;
- ограничения в части управления портфелем проектов (по бюджету, человеческим ресурсам и др.);
- структура и перечень категорий проектов портфеля;
- перечень показателей и параметров оценки проектов для каждой категории;
- перечень методик системного анализа и оценки проектов;
- перечень показателей портфеля проектов, отражающих степень их важности и инвестиционной привлекательности;
- нормативные документы, применяемые для управления портфелем проектов;
- перечень проектов, рекомендованных к реализации в рамках портфеля;
- перечень реализуемых проектов портфеля с их оценками;
- перечень потенциальных проектов портфеля с их приоритетностью;
- перечень проектов, не рекомендованных к включению в состав портфеля (отклоненные проекты, проекты, реализацию которых необходимо остановить, и иные неприоритетные проекты);
- результаты укрупненного распределения бюджета и ресурсов для одобренных проектов;
- отчеты об исполнении отдельных проектов и портфеля проектов в целом;
- запросы на изменения портфеля проектов;
- управленческие решения, включающие решения по внесению изменений в состав проектов портфеля, по изменению приоритетов проектов, по перераспределению ресурсов между проектами, по корректировке отдельных проектов, рекомендации по изменению методологии управления портфелем проектов.

6.1.3 Для получения выходных результатов процесса управления портфелем проектов в соответствии с принятыми в организации политиками и процедурами выполняют следующие основные действия:

- обеспечение управления портфелем проектов, включая:

- сбор информации об условиях, ограничениях и требованиях к портфелю проектов (информации о стратегических целях и приоритетах организации, об ограничениях по бюджету, человеческим и иным ресурсам, информации, влияющей на стратегические решения и управление организацией и портфелем проектов),

- определение новых или меняющихся областей деятельности, возможностей и рисков в деловой сфере, реализуемости и соответствия планов стратегии деловой деятельности организации,

- установление единой системы формальных методик, процедур и критериев для управления портфелем проектов;

- формирование портфеля проектов, включая:

- определение всех потенциальных проектов, сгруппированных по категориям, с указанием целей, задач и предполагаемых результатов проектов, рисков и возможных препятствий для выполнения проектов, оценок вероятностей успешности проектов, необходимых затрат и ожидаемых эффектов, определением и распределением ресурсов для достижения целей, определением взаимодействия и зависимости между проектами, определением отчетности и контрольных точек, формированием команд проектов и установлением ролей, ответственности, подотчетности и полномочий лиц в командах,

- определение и документирование перечня отклоненных проектов портфеля,

- уточнение и документирование перечня реализуемых в настоящий момент проектов портфеля, сгруппированных по категориям,

- определение и документирование перечня проектов, по которым требуется дополнительная информация для анализа;

- системный анализ портфеля проектов, включая:

- анализ степени продвижения проектов в направлении достижения конечных целей, соответствия действующим правовым и нормативным документам, принятым решениям, приказам и распоряжениям, выполнения планов и процедур в жизненном цикле систем для обеспечения их жизнеспособности,

- принятие решений по продолжению или переопределению проектов, которые удовлетворительно развиваются или смогут удовлетворительно развиваться в результате соответствующего переопределения,

- уточнение приоритетов проектов по интегральному показателю и/или в результате обоснованной необходимости для организации,

- оптимизацию и обеспечение сбалансированности портфеля проектов, обеспечивающей достижение стратегических целей организации наилучшим образом в условиях существующих ограничений (в том числе уточнение состава текущего портфеля проектов, распределения ресурсов и бюджета портфеля между проектами);

- мониторинг и контроль портфеля проектов, включая оперативное выявление отклонений текущих показателей от плановых и обеспечение корректирующих действий для их устранения, а также управление изменениями;

- завершение проектов, включая отмену или приостановку проектов, в которых риски для организации перевешивают выгоду от длительных инвестиций (если позволяют соглашения), а также закрытие проектов по завершении договоров.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процесса управления портфелем проектов, 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. приложение В).

### 6.2 Требования к составу показателей

Выбираемые показатели должны обеспечивать проведение оценки эффективности защиты информации и прогнозирования интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации.

Эффективность защиты информации оценивают с использованием количественных показателей, которые позволяют сформировать представление о текущих и потенциальных проблемах или о возмож-

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

### 6.3 Требования к количественным показателям рисков

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

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

6.3.2 Риск нарушения надежности реализации процесса управления портфелем проектов без учета требований по защите информации характеризуют соответствующей вероятностью нарушения надежности реализации процесса управления портфелем проектов (в зависимости от вероятности невыполнения необходимых действий процесса и вероятности нарушения сроков выполнения необходимых действий процесса) в сопоставлении с возможными ущербами.

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

6.3.4 Интегральный риск нарушения реализации процесса управления портфелем проектов характеризуют соответствующей вероятностью нарушения надежности реализации процесса без учета защиты информации и вероятностью нарушения требований по защите информации (см. В.2, В.3, В.4) в сопоставлении с возможными ущербами.

### 6.4 Требования к источникам данных

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

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

Типовые исходные данные для моделирования приведены в приложении В.

## 7 Требования к системному анализу

Требования к системному анализу процесса управления портфелем проектов включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению явных и скрытых угроз надежности реализации процесса и безопасности информации;
- требования к поддержке принятия решений в процессе управления портфелем проектов.

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

При обосновании и формулировании конкретных требований к системному анализу дополнительно руководствуются положениями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики проектов и организации, применяющей процесс управления портфелем проектов.

Примечание — Примеры решения задач системного анализа в приложении к различным процессам см. в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

**Приложение А**
**(справочное)**

## Пример перечня защищаемых активов

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

- выходные результаты процесса управления портфелем проектов — по 6.1.2;
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации — см. [21]—[24];
- договоры и соглашения на выполнение проектов и их составных частей;
- лицензии, подтверждающие право поставщиков (производителей) на выполнение проектов и их составных частей;
- финансовые и плановые документы, связанные с выполнением проектов;
- документацию при обследовании объекта автоматизации (для автоматизируемых систем) — по ГОСТ 34.601;
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101 с учетом специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем, связанных с проектами, входящими в портфель проектов;
- конструкторскую и технологическую документацию — по ГОСТ 2.051, ГОСТ 2.102, ГОСТ 3.1001, ГОСТ 34.201 с учетом специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем, связанных с проектами, входящими в портфель проектов;
- эксплуатационную и ремонтную документацию — по ГОСТ Р 2.601, ГОСТ 2.602, ГОСТ 34.201 с учетом специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем, связанных с проектами, входящими в портфель проектов;
- технические задания — по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602 с учетом специфики организации, применяющей процесс, а также специфики создаваемых (модернизируемых) и/или применяемых систем, связанных с проектами, входящими в портфель проектов;
- персональные данные, базу данных и базу знаний, систему хранения архивов по проектам;
- систему передачи данных и облачные данные организации, связанные с проектами;
- выходные результаты иных процессов в жизненном цикле систем, связанных с проектами (входящими в портфель проектов), с учетом их специфики.

**Приложение Б**
**(справочное)**

## Пример перечня угроз

Перечень угроз безопасности информации в процессе управления портфелем проектов может включать (в части, свойственной этому процессу):

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 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 — см. [21]—[24];
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124;
- угрозы безопасности информации при подготовке и обработке документов — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412;
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010 (приложение С), ГОСТ Р 59215;
- угрозы, связанные с приобретением или предоставлением облачных услуг для выполнения проектов (из портфеля проектов), которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги, — по ГОСТ Р ИСО/МЭК 27036-4;
- 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 соответствующим государственным регулятором.

**Приложение В**
**(справочное)**

## Типовые модели и методы прогнозирования рисков

### В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе управления портфелем проектов применяют любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Применение типовых методов и моделей настоящего стандарта обеспечивает оценку следующих показателей:

- риска нарушения надежности реализации процесса управления портфелем проектов без учета требований по защите информации — см. В.2;
- риска нарушения требований по защите информации в процессе управления портфелем проектов — см. В.3;
- интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации — см. В.4.

В.1.2 Риск нарушения надежности реализации процесса управления портфелем проектов без учета требований по защите информации характеризуют:

- риском невыполнения необходимых действий процесса, определяемым вероятностью невыполнения необходимых действий процесса;
- риском нарушения сроков выполнения необходимых действий, определяемым вероятностью нарушения сроков выполнения необходимых действий.

Риск нарушения требований по защите информации в процессе управления портфелем проектов определяют соответствующей вероятностью нарушения требований по защите информации.

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

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

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

В.1.5 Нарушение надежности реализации процесса управления портфелем проектов с учетом требований по защите информации характеризуется переходом в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по причинам: либо из-за невыполнения необходимых действий процесса, либо из-за нарушения сроков выполнения необходимых действий процесса, либо из-за нарушения требований по защите информации, либо из-за комбинации перечисленных причин.

В.1.6 В общем случае исходя из целей системного анализа риски оценивают на разных исходных данных. При использовании одних и тех же моделей для расчетов это может приводить к различным оценкам и интерпретациям рисков. Различия связаны с неодинаковой тяжестью возможного ущерба для заинтересованных сторон (из-за невыполнения необходимых действий процесса, нарушения сроков выполнения необходимых действий, нарушений требований по защите информации), недоступностью или неполнотой статистических данных, используемых каждой их этих сторон в качестве исходных данных при системном анализе.

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

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

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

В.1.8 При формировании исходных данных для моделирования и проведении разностороннего системного анализа используют статистические методы по ГОСТ Р ИСО 3534-2, методы оценки рисков из настоящего приложения и/или по ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1.

### В.2 Прогнозирование риска нарушения надежности реализации процесса без учета требований по защите информации

#### В.2.1 Общие положения

В.2.1.1 Надежность реализации процесса управления портфелем проектов без учета требований по защите информации представляет собой свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса с обеспечением сроков их выполнения.

В.2.1.2 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для анализируемого портфеля проектов или для портфеля проектов, выбранного в качестве аналога (портфеля-эталона). Для исследования запроектных сценариев развития угроз при моделировании могут быть использованы гипотетичные исходные данные.

В.2.1.3 Используется предположение, что нарушение надежности реализации процесса управления портфелем проектов без учета требований по защите информации является следствием невыполнения необходимых действий процесса и/или нарушения сроков выполнения необходимых действий процесса.

#### В.2.2 Оценка риска невыполнения необходимых действий процесса

В.2.2.1 Общие положения

Риск невыполнения необходимых действий процесса оценивают в качестве вспомогательного показателя при проведении оценок интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации — см. В.4.

В реализуемом процессе должны быть выполнены необходимые действия. Невыполнение (в т. ч. незавершение выполнения) необходимых действий процесса управления портфелем проектов — это угроза возможного ущерба. С точки зрения тяжести ущерба в случае невыполнения необходимых действий процесса все действия могут быть распределены по $k$ группам, $k \geq 1$ (при необходимости). В общем случае для каждой группы требования к выполнению процесса управления портфелем проектов формулируют на уровне инструкций должностных лиц, участвующих в реализации процесса.

В.2.2.2 Метод оценки

При оценке риска вычисляют вероятность невыполнения необходимых действий процесса управления портфелем проектов по отдельной группе действий или по всем действиям и делают сопоставление с возможным ущербом.

На основе применения статистических данных вероятность $R_{\text{действий } k}$ невыполнения необходимых действий процесса для $k$-й группы за задаваемое время $T_{\text{зад } k}$ вычисляют по формуле

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

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ — соответственно количество случаев нарушений при невыполнении необходимых действий процесса и общее количество необходимых действий из $k$-й группы, подлежащих выполнению за заданное время $T_{\text{зад } k}$ согласно статистическим данным.

Вероятность невыполнения необходимых действий процесса $R_{\text{действий}}$ по всему множеству действий согласно статистическим данным вычисляют по формулам:

- для варианта, когда учитывают все действия (как с завершенным выполнением, так и с их невыполнением)

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k [1 - R_{\text{действий } k}(T_{\text{зад } k})] / \sum_{k=1}^{K} W_k; \quad \text{(В.3)}$$

- для варианта, когда учитывают лишь те случаи, для которых необходимые действия процесса не были выполнены или завершены требуемым образом (именно они определяют возможные ущербы от невыполнения процесса)

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

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

$W_k$ — количество учитываемых действий из $k$-й группы при многократных реализациях процесса.

Для $k$-й группы учитывают требование к выполнению действий процесса с использованием индикаторной функцией $Ind(\alpha) = Ind_{\text{действий}}(\alpha_k)$.

Индикаторная функция $Ind\ (\alpha) = Ind_{\text{действий}}(\alpha_k)$ позволяет учесть последствия, связанные с невыполнением необходимых действий процесса, — см. формулу (В.1). Условие $\alpha_k$ означает совокупность условий выполнения в требуемом объеме и завершения всех действий процесса при соблюдении ограничений на задаваемое время $T_{\text{зад}\ k}$.

Примечания

1 При соблюдении всех условий вероятностные оценки рисков по формулам (В.3), (В.4) совпадают.

2 Практическая ценность расчетов применения формул (В.2)—(В.4) проявляется при общем количестве необходимых действий процесса $G_k\ (T_{\text{зад}\ k})$, подлежащих выполнению за заданное время $T_{\text{зад}\ k}$, не менее 10 и количестве случаев невыполнения необходимых действий процесса $G_{\text{наруш}\ k}\ (T_{\text{зад}\ k}) > 0$, $k = 1,\ldots,k$, $k \geq 1$. Тем самым считают подтвержденными практические условия повторяемости анализируемых событий. При невыполнении этих условий делают предположение о многократной повторяемости анализируемых событий и для расчетов используют адаптированные математические модели для прогнозирования рисков нарушения надежности реализации системных процессов — см., например В.3, ГОСТ Р 59341—2021 (В.3 приложения В), ГОСТ Р 59345—2021 (В.2 приложения В), ГОСТ Р 59347—2021 (В.2 приложения В).

**В.2.3 Оценка нарушения сроков выполнения необходимых действий процесса**

В.2.3.1 Общие положения

Вероятность нарушения сроков выполнения необходимых действий процесса в интересах системы оценивают в виде вспомогательного показателя при проведении оценок интегрального риска нарушения реализации процесса с учетом требований по защите информации — см. В.4.

Каждое осуществляемое действие, чтобы избежать ущербов, должно быть выполнено в задаваемые сроки. Нарушение сроков выполнения необходимых действий — это угроза потенциального ущерба (в т. ч. в виде упущенной выгоды). С точки зрения важности, срочности действий и тяжести ущерба в случае нарушения сроков выполнения необходимые действия могут быть условно распределены по $i$ группам, $i \geq 1$ (при необходимости). В общем случае для каждой группы требования к своевременности формулируют в виде: срок выполнения действий из $i$-й группы должен быть не более задаваемого $T_{\text{зад}\ i}$, $i = 1,\ldots,i$. Неприемлемость нарушения задаваемых сроков выполнения необходимых действий фиксируют в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение нарушений сроков выполнения действий в процессе управления портфелем проектов.

В.2.3.2 Метод оценки

При оценке риска вычисляют вероятность нарушения сроков выполнения действий процесса.

На основе применения статистических данных вероятность нарушения сроков выполнения для однократного действия из $i$-й группы $R_{\text{св}\ i}$ за задаваемое время $T_{\text{зад}\ i}$ вычисляют по формуле

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

где $N_{\text{наруш}\ i}\ (T_{\text{зад}\ i})$ и $N_i\ (T_{\text{зад}\ i})$ — соответственно количество случаев нарушений сроков выполнения необходимых действий и общее количество действий процесса за заданное время множества действий из $i$-й группы $T_{\text{зад}\ i}$ согласно статистическим данным.

Вероятность нарушения сроков выполнения необходимых действий по всему множеству действий процесса, реализуемых в процессе согласно статистическим данным, вычисляют по формулам:

- для варианта, когда учитывают все действия (как с выполненными, так и с нарушенными сроками их выполнения):

$$R_{\text{св}}(T_{\text{зад}}) = 1 - \sum_{i=1}^{I} M_i [1 - R_{\text{св}\ i}(T_{\text{зад}\ i})] / \sum_{i=1}^{I} M_i; \tag{В.6}$$

- для варианта,когда учитывают лишь те случаи, для которых сроки выполнения действий были нарушены (именно они определяют возможные ущербы от несвоевременного выполнения действий):

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

где $T_{\text{зад}}$ — задаваемое суммарное время для выполнения всех действий, включающее в себя все частные значения $T_{\text{зад}\ i}$ с учетом их наложений;

$M_i$ — количество учитываемых действий при многократных выполнениях процесса.

Для действий из $i$-й группы учитывают требование к срокам их выполнения с использованием индикаторной функцией $Ind\ (\alpha) = Ind_{\text{св}}\ (\alpha_i)$. Индикаторная функция $Ind\ (\alpha) = Ind_{\text{св}}\ (\alpha_i)$ позволяет учесть последствия, связанные с

несвоевременностью выполнения действий процесса. Условие $\alpha_j$ означает совокупность условий по ограничениям на задаваемые сроки $T_{зад\,i}$.

Примечания

1 При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.6), (В.7) совпадают.

2 Практическая ценность расчетов применения формул (В.5)—(В.7) проявляется при общем количестве действий процесса $N_j(T_{зад\,i})$ за заданное время $T_{зад\,i}$ не менее 10 и количестве случаев нарушений сроков выполнения необходимых действий $N_{наруш\,i}(T_{зад\,i}) > 0$, $i = 1,...,I$, $I \geq 1$. Тем самым считают подтвержденными практические условия повторяемости анализируемых событий. При невыполнении этих условий делают предположение о многократной повторяемости анализируемых событий и для расчетов используют адаптированные математические модели для прогнозирования рисков — см., например, В.3, ГОСТ Р 59341—2021 (В.3 приложения В), ГОСТ Р 59345—2021 (В.2 приложения В), ГОСТ Р 59347—2021 (В.2 приложения В).

### В.3 Прогнозирование риска нарушения требований по защите информации

#### В.3.1 Общие положения

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

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

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

В.3.1.4 Для математической формализации используют следующие основные положения:

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

Под целостностью моделируемой системы понимается такое ее состояние, которое в течение задаваемого периода прогноза отвечает целевому назначению модели системы. В данном случае непосредственно процесс управления портфелем проектов может быть рассмотрен в качестве моделируемой системы. При моделировании, направленном на прогнозирование риска нарушения требований по защите информации, целевое назначение моделируемой системы проявляется в выполнении требований по защите информации. Такая интерпретация подразумевает выполнение требований по защите информации не только применительно к защищаемым активам и действиям, с использованием которых создают и получают выходные результаты, но и к самим выходным резуль-

татам, которые применяют (или планируют к созданию, получению и/или применению). В итоге для каждого из элементов и моделируемой системы в целом в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных состояний на временной оси образуют два основных состояния:

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

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение успешной реализации процесса управления портфелем проектов.

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

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

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

**В.3.2 Исходные данные и расчетные показатели**

Для расчета вероятностных показателей применительно к процессу управления портфелем проектов, где анализируемые сущности (выходные результаты, действия) могут быть представлены в виде системы — «черного ящика», используют исходные данные, формально определяемые в общем случае следующим образом:

$\sigma$ — частота возникновения источников угроз нарушения требований по защите информации в процессе управления портфелем проектов;

$\beta$ — среднее время развития угроз с момента возникновения источников угроз до нарушения нормальных условий реализации процесса (например, до нарушения установленных требований по защите информации или до инцидента);

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

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

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

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

Расчетные показатели:

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

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

Расчет показателей применительно к процессу управления портфелем проектов для моделируемой системы простой и сложной структуры осуществляют по формулам ГОСТ Р 59341—2021 (В.2 приложения В).

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

**В.4 Прогнозирование интегрального риска**

**В.4.1 Общие положения**

Прогнозирование интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации применяют при решении задач системного анализа — см. раздел 7.

Интегральный риск оценивают с использованием расчетных вероятностей невыполнения необходимых действий процесса, нарушения сроков выполнения необходимых действий процесса (см. В.2) и нарушения требований по защите информации (см. В.3) в сопоставлении с возможными ущербами.

**В.4.2 Метод оценки**

Вероятность нарушения надежности реализации процесса управления портфелем проектов без учета требований по защите информации вычисляют по формулам:

- для варианта, когда учитывают все действия (как с выполненными, так и с нарушенными условиями по выполнению необходимых действий процесса и соблюдению сроков их выполнения):

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - \left\{\sum_{k=1}^{K} W_k [1 - R_{\text{действий}\,k}(T_{\text{зад},k})] + \sum_{i=1}^{I} M_i [1 - R_{\text{сш}\,i}(T_{\text{зад},i})]\right\} / \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i\right); \quad \text{(В.8)}$$

- для варианта, когда учитывают лишь те случаи, для которых условия по выполнению необходимых действий процесса и/или соблюдению сроков их выполнения были нарушены (именно они определяют возможные ущербы)

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - \left\{\sum_{k=1}^{K} W_k [1 - R_{\text{действий}\,k}(T_{\text{зад},k})] \ln z'_{\text{действий}}(a_k) + \sum_{i=1}^{I} M_i [1 - R_{\text{сш}\,i}(T_{\text{зад},i})] \ln z'_{\text{сш}}(a_i)\right\} / \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i\right), \quad \text{(В.9)}$$

где $T_{\text{зад}}$ — задаваемое общее время для выполнения всех действий, включающее в себя все частные значения $T_{\text{зад}\,k}$, $T_{\text{зад}\,i}$ с учетом их наложений — см. формулы (В.2)—(В.9).

Примечание — При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.8), (В.9) совпадают.

Интегральную вероятность нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации $R_{\text{интегр.уч}}(T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле

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

Здесь вероятность нарушения надежности реализации процесса в течение периода прогноза без учета требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$ рассчитывают по формулам (В.8) и/или (В.9) в зависимости от целей системного анализа. Вероятность нарушения требований по защите информации в системе в течение периода прогноза $R_{\text{наруш}}(T_{\text{зад}})$ рассчитывают по рекомендациям подраздела В.3 для выбранной при проведении системного анализа структуры моделируемой системы.

Интегральный риск нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации определяют путем сопоставления расчетной вероятности нарушения реализации процесса в течение периода прогноза, рассчитанной по формуле (В.10), с возможным ущербом за этот период.

Примечание — Примеры прогнозирования рисков в приложении к различным процессам см. в ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

**Приложение Г**
**(справочное)**

## Типовые допустимые значения показателей рисков для процесса управления портфелем проектов

С точки зрения остаточного риска, характеризующего приемлемый уровень целостности рассматриваемого портфеля проектов, предъявляемые требования системной инженерии подразделяют на требования при допустимых рисках, обосновываемых по прецедентному принципу согласно ГОСТ Р 59349, и требования при рисках, свойственных реальному или гипотетичному портфелю-эталону. При формировании требований системной инженерии необходимо обоснование достижимости целей проектов, входящих в портфель, и рассматриваемого процесса управления портфелем проектов, 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 проектов, ограничения на условия их реализации, указывают другие условия в зависимости от специфики проектов и организаций, их выполняющих.

Требования системной инженерии при принимаемых рисках, свойственных портфелю-эталону, являются наиболее жесткими, они не учитывают специфики рассматриваемых проектов, 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 подлежат каждый проект, входящий в портфель, и связанные с ним системы, составляющие их подсистемы и реализуемые процессы жизненного цикла. Выполнение этих требований является гарантией обеспечения высокого качества и безопасности рассматриваемого портфеля проектов. Вместе с тем проведение работ системной инженерии с ориентацией на риски, свойственные портфелю-эталону, характеризуются существенно большими затратами по сравнению с требованиями, ориентируемыми на допустимые риски, обосновываемые по прецедентному принципу. Это заведомо удорожает проекты, увеличивает время до их завершения и принятия в эксплуатацию связанных с этими проектами систем.

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

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

Таблица Г.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 портфелем проектов | Не выше 0,10 | Не выше 0,05 |
| Интегральный риск нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации | Не выше 0,10 | Не выше 0,05 |

**Приложение Д**
**(справочное)**

## Примерный перечень методик системного анализа для процесса управления портфелем проектов

Д.1 Методика прогнозирования риска нарушения требований по защите информации в процессе управления портфелем проектов.

Д.2 Методика прогнозирования интегрального риска нарушения реализации процесса управления портфелем проектов с учетом требований по защите информации и возможных ущербов.

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

Д.4 Методики выявления явных и скрытых недостатков процесса управления портфелем проектов с использованием прогнозирования рисков.

Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления портфелем проектов и противодействие угрозам нарушения требований по защите информации.

Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления портфелем проектов.

Примечания

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

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

## Библиография


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ключевые слова: актив, безопасность, защита информации, модель, процесс управления портфелем проектов, риск, система

Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 29.04.2021. Подписано в печать 13.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.

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