ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59329— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССАХ ПРИОБРЕТЕНИЯ И ПОСТАВКИ ПРОДУКЦИИ И УСЛУГ ДЛЯ СИСТЕМЫ

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 апреля 2021 г. № 305-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 4
4 Основные положения системной инженерии по защите информации в процессах приобретения и поставки 6
5 Общие требования системной инженерии по защите информации в процессах приобретения и поставки 7
6 Специальные требования к количественным показателям 9
7 Требования к системному анализу 11
Приложение А (справочное) Пример перечня защищаемых активов 12
Приложение Б (справочное) Пример перечня угроз 13
Приложение В (справочное) Типовые модели и методы прогнозирования рисков для процессов приобретения и поставки 14
Приложение Г (справочное) Типовые допустимые значения показателей рисков для процессов приобретения и поставки 22
Приложение Д (справочное) Примерный перечень методик системного анализа для процессов приобретения и поставки 23
Библиография 24

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 настоящему стандарту;
- для процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, управления инфраструктурой системы, управления портфелем, управления человеческими ресурсами, управления качеством, управления знаниями — по ГОСТ Р 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335;
- для процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, управления рисками, управления конфигурацией, управления информацией, измерений, гарантии качества — по ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343;
- для технических процессов — процессов анализа бизнеса или назначения, определения 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 процессах приобретения и поставки продукции и услуг для системы и специальные требования к используемым количественным показателям.

Для планируемых и реализуемых процессов приобретения и поставки продукции и услуг для системы применение настоящего стандарта при создании (модернизации, развитии), эксплуатации систем и выведении их из эксплуатации обеспечивает проведение системного анализа, основанного на прогнозировании рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССАХ ПРИОБРЕТЕНИЯ И ПОСТАВКИ ПРОДУКЦИИ И УСЛУГ ДЛЯ СИСТЕМЫ

System engineering. Protection of information in production and services acquisition and supply processes for system

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа процессов приобретения и поставки продукции и услуг для систем различных областей приложения применительно к вопросам защиты информации.

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

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

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процессы приобретения и поставки продукции и услуг для системы, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем, — см. примеры систем в [1]—[26].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.051 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 15.301 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

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

ГОСТ Р ИСО/МЭК 27036-2 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования

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

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

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

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

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

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

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

ГОСТ Р 59333 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 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 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

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 59330, ГОСТ Р 59331, ГОСТ Р 59332, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59340, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59343, ГОСТ Р 59344, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357, ГОСТ Р МЭК 61508-4, а также следующие термины с соответствующими определениями:

3.1.1

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.2

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

[ГОСТ Р 50922—2006, статья 2.1.1]

3.1.3

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

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

[ГОСТ Р 50922—2006, статья 2.3.2]

3.1.4

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

[ГОСТ Р 50922—2006, статья 2.3.3]

3.1.5

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

[ГОСТ Р 50922—2006, статья 2.3.4]

3.1.6 **интегральный риск нарушения реализации процесса приобретения или поставки продукции и/или услуг для системы с учетом требований по защите информации:** Сочетание вероятности того, что будут нарушены надежность реализации процесса либо требования по защите информации, либо и то и другое, с тяжестью возможного ущерба.

3.1.7 **надежность реализации процесса приобретения или поставки продукции и/или услуг для системы:** Свойство процесса сохранять во времени в установленных пределах значения показателей процесса, характеризующих способность выполнить процесс в заданных условиях его реализации с обеспечением сроков поставки и качества приобретаемых (или поставляемых) продукции и/или услуг.

3.1.8

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.9

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.10

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.11

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]

3.1.12 **система-эталон:** Реальная или гипотетичная система, которая по своим показателям интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации принимается в качестве эталона для полного удовлетворения требований заинтересованных сторон системы и 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.

3.1.13

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]

3.1.14

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]

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

3.1.16

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 процессах приобретения и поставки

4.1 Общие положения

Организации используют процесс приобретения для того, чтобы приобретать, а процесс поставки — чтобы поставлять требуемые продукцию и/или услуги для системы. При планировании и реализации процессов приобретения и поставки продукции и услуг для системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Для прогнозирования рисков, связанных с реализацией процессов, и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах используют системный анализ процессов с учетом требований по защите информации в условиях возможных угроз. Определение выходных результатов процессов приобретения и поставки продукции и услуг для системы и типовых действий по защите информации, применимых к отношениям поставщика и приобретающей стороны, осуществляют по ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р 57102, ГОСТ Р 57193. Оценку интегральных рисков нарушения реализации процессов приобретения и/или поставки продукции и/или услуг для системы с учетом требований по защите информации осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р 57102, ГОСТ Р 59215. При этом учитывают специфику создаваемой (модернизируемой) и/или применяемой системы — см., например, [20]—[26].

4.2 Цели процессов и назначение мер защиты информации

4.2.1 Определение целей процессов приобретения и поставки продукции и услуг для системы осуществляют по ГОСТ 34.601, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1 с учетом специфики организации, применяющей процесс. В общем случае целями процессов являются надежная реализация приобретения или поставки для системы продукции и/или услуг заданного качества в заданные сроки согласно условиям соглашений приобретающей стороны и поставщика.

4.2.2 Меры защиты информации в процессах приобретения продукции и услуг для системы предназначены для обеспечения конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамерен-

ных воздействий на защищаемую информацию. Определение мер защиты информации осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 58412, ГОСТ Р 59215 с учетом специфики создаваемой (модернизируемой) или применяемой системы — см., например, [21] — [24].

4.3 Стадии и этапы жизненного цикла системы

Процессы приобретения и поставки продукции и услуг для системы могут быть использованы на любой стадии жизненного цикла системы. Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации системы устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1.

Процессы приобретения и/или поставки продукции и/или услуг для системы могут входить в состав работ, выполняемых в рамках других процессов жизненного цикла систем, и при необходимости включать в себя другие процессы.

4.4 Основные принципы

При проведении системного анализа процессов приобретения и поставки продукции и услуг для системы руководствуются основными принципами, определенными в ГОСТ Р 59349 с учетом дифференциации требований по защите информации в зависимости от категории значимости системы и важности обрабатываемой в ней информации (см. ГОСТ Р 59346, [20]—[26]). Все применяемые принципы подчинены принципу целенаправленности осуществляемых действий.

4.5 Основные усилия системной инженерии

Основные усилия системной инженерии для обеспечения защиты информации в каждом из процессов приобретения или поставки продукции или услуг для системы сосредотачивают:

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

5 Общие требования системной инженерии по защите информации в процессах приобретения и поставки

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на разработку, модернизацию или развитие системы, ТЗ на приобретение и поставку продукции и/или услуг для системы. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы (в качестве которой может выступать система защиты информации), в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований по защите информации формируют при выполнении процесса определения системных требований с учетом нормативных и правовых документов Российской Федерации (см., например, [1]—[26]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов — см. ГОСТ Р 59346.

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

5.2 Требования системной инженерии призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации процессов приобретения и поставки продукции и услуг для системы и поддержке при этом эффективности защиты информации.

Требования системной инженерии по защите информации в процессах приобретения и поставки продукции и услуг для системы включают:

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

5.3 Состав выходных результатов и выполняемых действий в процессах приобретения и поставки продукции и услуг для системы определяют по ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 59215 с учетом специфики создаваемой (модернизируемой) и/или применяемой системы.

5.4 Меры защиты информации и действия по защите информации должны охватывать активы, информация которых или о которых подлежит защите для получения выходных результатов и выполнения процессов приобретения и поставки продукции и услуг для системы.

Примечание — В состав активов могут быть включены активы иных систем (подсистем), не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика например привлекаемые средства контроля качества поставляемой продукции у поставщика.

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.201, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом требований ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 20000-1, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 59215, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2 с учетом специфики системы (см., например, [21]—[26]).

Примеры перечней учитываемых активов и угроз в процессах приобретения и поставки продукции и услуг для системы приведены в приложениях А и Б.

5.6 Эффективность защиты информации при выполнении процессов приобретения и поставки продукции и услуг для системы анализируют по показателям рисков в зависимости от специфики системы, целей ее применения и возможных угроз. В системном анализе процессов используют модель угроз безопасности информации.

Системный анализ процессов осуществляют с использованием методов, моделей и методик (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р 58771, [21]—[26].

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 процессов приобретения и поставки продукции и/или услуг для системы определен в 6.3.

Типовые модели, методы и указания по прогнозированию рисков применительно к процессам приобретения и поставки продукции и/или услуг для системы, допустимые значения для расчетных показателей и примерный перечень методик системного анализа приведены в приложениях В, Г, Д. Характеристики мер и действий по защите информации и исходные данные, обеспечивающие применение моделей, методов 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, осуществляемым действиям, выходным результатам, к которым предъявлены определенные требования по защите информации, выполняют оценку эффективности защиты информации на основе прогнозирования рисков в условиях возможных угроз. Для обоснования эффективных предупреждающих мер и действий по снижению рисков или их удержанию в допустимых пределах используют системный анализ.

6.1.2 Основными выходными результатами процесса приобретения продукции и/или услуг для системы являются:

- запросы на поставку продукции и/или услуг;
- результаты выбора одного или более поставщиков;
- соглашение между приобретающей стороной и поставщиком;
- принимаемые продукция и/или услуги, соответствующие соглашению;
- документы, определенные в соглашении, о приемке поставленных продукции и/или услуг, включая принятие приобретающей стороной ответственности за приобретенные продукцию или услуги.

Основными выходными результатами процесса поставки продукции и/или услуг для системы являются:

- ответ на запрос приобретающей стороны на поставку продукции и/или услуг;
- соглашение между приобретающей стороной и поставщиком;
- поставленные продукция и/или услуги, соответствующие соглашению;
- документы, определенные в соглашении, о приемке поставленных продукции и/или услуг, включая передачу приобретающей стороне ответственности за приобретенные продукцию или услуги.

6.1.3 Для получения выходных результатов процесса приобретения продукции и/или услуг в общем случае выполняют следующие основные действия:

- подготовку к приобретению, включая:
  - определение стратегии приобретения, предусматривающей уменьшение различных рисков, задание контрольных точек и сроков в приобретении продукции и/или услуг, формирование критериев выбора поставщика;
  - подготовку запроса на поставку продукции и/или услуг, который включает конкретные требования заинтересованных сторон и/или системные требования к поставляемым продукции и/или услугам;
- доведение до поставщиков намерений о приобретении продукции и/или услуг и выбор поставщика;
- заключение соглашения между приобретающей стороной и поставщиком, предусматривающего удовлетворение конкретных требований заинтересованных сторон и/или системных требований к поставляемым продукции и/или услугам, контрольные сроки разработок и поставок, условия верификации, приемки, аттестации и процедуры обработки исключительных ситуаций, процедуры контроля и оценки изменений и графики оплаты получаемых продукции и/или услуг;
- контроль выполнения соглашения, включая необходимые оценки, изменения и информирование согласно условиям соглашения;
- выполнение соглашения с получением поставляемых продукции и/или услуг, подтверждение соответствия соглашению, обеспечение оплаты или других согласованных действий в соответствии с соглашением, закрытие соглашения.

Для получения выходных результатов процесса поставки продукции и/или услуг в общем случае выполняют следующие основные действия:

- подготовку к поставке, включая:
  - определение существования и основных характеристик приобретающей стороны;
  - определение стратегии поставки, предусматривающей уменьшение различных рисков, задание контрольных точек и сроков в поставке продукции и/или услуг;
- ответ на запрос, поступивший на поставку продукции и/или услуг, включая предварительную оценку его выполнимости;
- заключение соглашения между приобретающей стороной и поставщиком, предусматривающего удовлетворение конкретных требований заинтересованных сторон и/или системных требований к поставляемым продукции и/или услугам, контрольные сроки разработок и поставок, условия верифика-

ции, приемки, аттестации и процедуры обработки исключительных ситуаций, процедуры контроля и оценки изменений, графики оплаты поставляемых продукции и/или услуг;

- контроль выполнения соглашения, включая необходимые оценки, изменения и информирование согласно условиям соглашения;

- выполнение соглашения с поставкой продукции и/или услуг, подтверждение соответствия соглашению, получение оплаты или выполнение других согласованных действий в соответствии с соглашением, закрытие соглашения.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по защите информации и нарушениями надежности реализации процессов приобретения и поставки продукции и услуг для системы, 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 рассматриваемого процесса приобретения или поставки продукции и/или услуг с учетом требований по защите информации.

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

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе приобретения и/или поставки продукции и/или услуг для системы используют следующие количественные показатели:

- риск нарушения надежности реализации процесса приобретения продукции и/или услуг для системы без учета требований по защите информации;

- риск нарушения требований по защите информации в процессе приобретения продукции и/или услуг для системы;

- риск нарушения надежности реализации процесса поставки продукции и/или услуг для системы без учета требований по защите информации;

- риск нарушения требований по защите информации в процессе поставки продукции и/или услуг для системы;

- интегральный риск нарушения реализации процесса приобретения продукции и/или услуг для системы с учетом требований по защите информации;

- интегральный риск нарушения реализации процесса поставки продукции и/или услуг для системы с учетом требований по защите информации.

6.3.2 Риск нарушения надежности реализации каждого из процессов приобретения или поставки продукции и/или услуг без учета требований по защите информации характеризуется соответствующей вероятностью в зависимости от нарушения надежности реализации процесса приобретения или поставки в сопоставлении с возможным ущербом.

6.3.3 Риск нарушения требований по защите информации в каждом из процессов приобретения или поставки продукции и/или услуг для системы 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 каждого из процессов приобретения или поставки продукции и/или услуг с учетом требований по защите информации характеризуют сочетанием вероятности нарушения надежности реализации процесса приобретения или поставки продукции и/или услуг без учета требований по защите информации с соответствующей вероятностью нарушения

требований по защите информации (см. В.2, В.3, В.4) в сопоставлении с возможным ущербом для системы.

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессам приобретения и поставки продукции и/или услуг для системы):

- временные данные функционирования системы защиты информации, в том числе срабатывания ее исполнительных механизмов;
- текущие и статистические данные о состоянии параметров системы защиты информации (привязанные к временам изменения состояний);
- текущие и статистические данные о самой системе или системах-аналогах, характеризующие не только данные о нарушениях надежности реализации процесса, но и события, связанные с утечкой защищаемой информации, несанкционированными или непреднамеренными воздействиями на защищаемую информацию (привязанные к временам наступления событий, характеризующих нарушения и предпосылки к нарушениям требований по защите информации);
- текущие и статистические данные результатов технического диагностирования системы защиты информации;
- наличие и готовность персонала системы защиты информации, данные об ошибках персонала (привязанные к временам наступления событий, последовавших из-за этих ошибок и характеризующих нарушения и предпосылки к нарушениям требований по защите информации) в самой системе или в системах-аналогах;
- данные 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 каждого из процессов приобретения или поставки продукции и/или услуг для системы 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 процессах приобретения и/или поставки продукции и/или услуг для системы.

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

При обосновании и формулировании конкретных требований к системному анализу процессов приобретения и/или поставки продукции и/или услуг для системы дополнительно руководствуются положениями ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, 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 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2 с учетом специфики создаваемой (модернизируемой) и/или применяемой системы — см., например, [21]—[26].

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 процессах приобретения и поставки продукции и услуг для системы может включать (в части, свойственной этим процессам):

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

Приложение Б
(справочное)

Пример перечня угроз

Перечень угроз безопасности информации в процессах приобретения и поставки продукции и услуг для системы может включать (в части, свойственной этим процессам):

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р 51275, ГОСТ Р 59215;
- угрозы государственным информационным системам, информационным системам персональных данных, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимым объектам критической информационной инфраструктуры Российской Федерации — по [21]—[24];
- угрозы безопасности функционирования программного обеспечения, оборудования и коммуникаций, используемых в процессе работы, — по ГОСТ Р ИСО/МЭК 27002 и ГОСТ Р 54124;
- угрозы возникновения уязвимостей в рамках цепи поставок, угрозы, связанные с отсутствием наглядности, прозрачности и прослеживаемости, а также управлением физически рассредоточенными многоуровневыми цепями поставок (например, поставок информационно-коммуникационных технологий), — по ГОСТ Р 59215;
- угрозы, связанные с глобальной цепью поставок для продукции и услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти продукцию и услуги (например, наличие контрафактной продукции информационно-коммуникационных технологий), — по ГОСТ Р 59215;
- угрозы компрометации информационной безопасности приобретающей стороны, угрозы возникновения ущерба репутации и/или потери доверия поставщика к конкретному заказчику, информация и информационные системы которого были скомпрометированы, — по ГОСТ Р 59215;
- угрозы, связанные с приобретением или предоставлением облачных услуг, 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 государственным регулятором.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков для процессов приобретения и поставки

В.1 Общие положения

В.1.1 В процессах приобретения и поставки продукции и услуг для системы применяют любые возможные модели и методы прогнозирования рисков, обеспечивающие приемлемое достижение поставленных целей. С учетом набираемой статистики типовые модели и методы прогнозирования рисков, излагаемые в настоящем стандарте, обеспечивают оценку следующих показателей согласно 6.3:

- рисков нарушения надежности реализации процессов приобретения и/или поставки продукции и/или услуг для системы без учета требований по защите информации — см. В.2;
- рисков нарушения требований по защите информации в процессах приобретения и/или поставки продукции и/или услуг для системы — см. В.3;
- интегральных рисков нарушения реализации процессов приобретения и/или поставки продукции и/или услуг для системы с учетом требований по защите информации — см. В.4.

В.1.2 Риск нарушения надежности реализации каждого из процессов приобретения или поставки продукции и/или услуг для системы без учета требований по защите информации характеризуют:

- риском невыполнения необходимых действий процесса, определяемым соответствующей вероятностью невыполнения необходимых действий процесса;
- риском нарушения сроков поставки, определяемым соответствующей вероятностью нарушения сроков выполнения необходимых действий;
- риском наличия недопустимого брака в поставляемых продукции и/или услугах для системы, определяемым соответствующей вероятностью наличия недопустимого брака в поставляемых продукции и/или услугах.

Риск нарушения требований по защите информации в каждом из процессов приобретения или поставки продукции и/или услуг для системы 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 каждого из процессов приобретения или поставки продукции и/или услуг для системы с учетом требований по защите информации характеризуют сочетанием риска нарушения надежности реализации процесса без учета требований по защите информации и риска нарушения требований по защите информации в соответствующем процессе.

В.1.4 При оценке рисков расчетные вероятностные показатели сопоставляют с возможным ущербом, оцениваемым тяжестью последствий для системы и ее заинтересованных сторон в случае реализации угроз.

В.1.5 Для моделируемой системы нарушение реализации каждого из процессов приобретения или поставки продукции и/или услуг с учетом требований по защите информации характеризуется переходом системы в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: либо из-за невыполнения необходимых действий процесса, либо из-за нарушения сроков поставки, либо из-за наличия недопустимого брака в поставляемых продукции и/или услугах, 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 поставки, наличия брака в поставляемой продукции и/или услугах, нарушений требований по защите информации), недоступностью или неполнотой статистических данных, используемых в качестве исходных данных при системном анализе.

В.1.7 Для выделяемых типов продукции и/или услуг выполнение или невыполнение действий и требований при моделировании отслеживается с использованием индикаторной функции $Ind\ (\alpha)$, которая позволяет учесть критичность последствий, связанных с невыполнением заданных условий согласно собираемой статистике:

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

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

В.1.8 При формировании исходных данных для моделирования и проведении разностороннего системного анализа используют методы оценки рисков из настоящего приложения или иные приемлемые методы — см., например, ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59349, ГОСТ Р МЭК 61069-1, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2.

В.2 Прогнозирование рисков нарушения надежности реализации процессов без учета требований по защите информации

В.2.1 Общие положения

В.2.1.1 Надежность реализации каждого из процессов приобретения или поставки продукции и/или услуг 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 поставки и качества поставляемых продукции и/или услуг.

В.2.1.2 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для анализируемой системы или для системы, выбранной в качестве аналога. Для исследования запроектных сценариев развития угроз при моделировании могут быть использованы гипотетичные исходные данные.

В.2.1.3 Надежность реализации каждого из процессов приобретения или поставки продукции и/или услуг без учета требований по защите информации характеризуют показателями:

- риском невыполнения необходимых действий процесса;
- риском нарушения сроков поставки;
- риском наличия недопустимого брака в поставляемых продукции и/или услугах.

В.2.1.4 Используется предположение, что нарушение надежности реализации каждого из процессов приобретения или поставки продукции и/или услуг для системы без учета требований по защите информации является следствием невыполнения необходимых действий процесса, и/или нарушения сроков выполнения необходимых действий процесса, и/или наличия недопустимого брака в поставляемых продукции и/или услугах.

Методические положения изложены в В.2.2—В.2.4 в обобщенном виде, применимом к любому из процессов приобретения или поставки продукции и/или услуг для системы.

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 каждого из процессов приобретения или поставки продукции и/или услуг для системы с учетом требований по защите информации — см. В.4.

В реализуемом процессе должны быть выполнены необходимые действия. Невыполнение (в том числе незавершение выполнения) необходимых действий процесса приобретения или поставки продукции и/или услуг — это угроза возможного ущерба. С точки зрения тяжести ущерба в случае невыполнения необходимых действий процесса поставляемые для системы продукция и/или услуги могут быть условно сгруппированы по K типам, $K \geq 1$. В общем случае для каждого типа требования к выполнению процессов приобретения или поставки продукции и/или услуг для системы формулируют на уровнях технической политики организации, требований заинтересованных сторон и полномочий должностных лиц, участвующих в реализации процессов.

В.2.2.2 Метод оценки

При оценке рисков вычисляют вероятность невыполнения необходимых действий процесса приобретения или поставки по отдельной группе продукции и/или услуг или по всему множеству типов продукции и/или услуг и делают сопоставление с возможным ущербом.

На основе применения статистических данных вероятность $R_{\text{действий } k}$ невыполнения необходимых действий рассматриваемого процесса приобретения или поставки продукции и/или услуг k-го типа за задаваемое время $T_{\text{зад } k}$ вычисляют по формуле

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

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ — соответственно количество случаев невыполнения необходимых действий процесса и общее количество необходимых действий процесса, подлежавших выполнению за заданное время $T_{\text{зад } k}$ для продукции и/или услуг k-го типа согласно статистическим данным.

Вероятность невыполнения необходимых действий процесса $R_{\text{действий}}(T_{\text{зад}})$ по всему множеству продукции и/или услуг различных типов согласно статистическим данным вычисляют по формулам:

- для случая, когда учитывают все поставки (как с завершенным выполнением всех необходимых действий процесса, 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 случая, когда учитывают лишь те поставки, для которых необходимые действия процесса не были выполнены или завершены требуемым образом (именно они являются причиной возможных ущербов)

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

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

W_k — количество учитываемых поставок продукции и/или услуг k-го типа при многократных поставках.

Для продукции и/или услуг k-го типа учитывают требование к выполнению действий процесса с использованием индикаторной функциии $Ind(\alpha) = Ind_{\text{действий}}(\alpha_k)$. Индикаторная функция $Ind(\alpha) = Ind_{\text{действий}}(\alpha_k)$ позволяет учесть последствия, связанные с невыполнением необходимых действий процесса, — см. формулу (В.4). Условие α_k означает совокупность условий выполнения в требуемом объеме и завершения всех необходимых действий процесса за задаваемый период времени $T_{\text{зад } k}$.

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, а также ГОСТ Р 59331—2021 (В.2 приложения В), ГОСТ Р 59341—2021 (В.3 приложения В), ГОСТ Р 59347—2021 (В.2 приложения В).

В.2.3 Оценка нарушения сроков поставки продукции и/или услуг

В.2.3.1 Общие положения

Вероятность нарушения сроков поставки продукции и/или услуг для системы оценивают в виде вспомогательного показателя при проведении оценок интегрального риска нарушения реализации рассматриваемого процесса с учетом требований по защите информации — см. В.4.

Чтобы избежать ущербов, каждая поставка продукции и/или услуг для системы (в том числе поставка промежуточных результатов внутри системы) должна быть выполнена в задаваемые сроки. Нарушение сроков поставки — это угроза возможного ущерба. С точки зрения важности, срочности действий и тяжести ущерба в случае нарушения сроков поставки поставляемые продукция и/или услуги могут быть условно сгруппированы по I типам, $I \geq 1$. В общем случае для каждого типа требования к своевременности поставки продукции и/или услуг формулируют в виде: срок поставки продукции и/или услуг i-го типа должен быть не более задаваемого $T_{\text{зад } i}$, $i = 1,\ldots, I$. Неприемлемость нарушения задаваемых сроков поставки фиксируют в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на соблюдение задаваемых сроков в процессе приобретения или поставки продукции и/или услуг для системы.

В.2.3.2 Метод оценки

При оценке конкретного риска вычисляют вероятность нарушения сроков однократной и множественных поставок для разнородных продукции и/или услуг.

На основе применения статистических данных вероятность $R_{\text{св } i}$ нарушения сроков выполнения однократной поставки для продукции и/или услуг i-го типа за задаваемое время $T_{\text{зад } i}$ вычисляют по формуле

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

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

Вероятность $R_{\text{св}}(T_{\text{зад}})$ нарушения сроков поставки по всему множеству продукции и/или услуг различных типов, реализуемых в анализируемом процессе согласно статистическим данным с учетом множественности поставок, характеризуемых исходными данными по каждому из типов продукции и/или услуг, вычисляют по формулам:

- для случая,когда учитывают все поставки (как с соблюдением, так и с нарушением сроков поставки)

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

- для случая, когда учитывают лишь те поставки, для которых сроки поставки были нарушены (именно они являются причиной возможных ущербов)

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

где $T_{зад}$ — задаваемое общее время для поставки всего множества продукции и/или услуг различных типов, включающее в себя все частные значения $T_{зад\,i}$ с учетом их наложений;

M_i — количество учитываемых поставок продукции и/или услуг i-го типа при многократных поставках.

Для продукции и/или услуг i-го типа учитывают ограничения на сроки поставки с использованием индикаторной функции $Ind(\alpha) = Ind_{св}(\alpha_i)$. Индикаторная функция $Ind(\alpha) = Ind_{св}(\alpha_i)$ позволяет учесть последствия, связанные с несоблюдением сроков поставок. Условие α_i означает соблюдение установленных сроков поставки для продукции и/или услуг i-го типа.

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 поставок $N_i(T_{зад\,i})$за заданное время $T_{зад\,i}$ не менее 10 и количестве случаев нарушений сроков поставки $N_{наруш\,i}(T_{зад\,i}) > 0$, $i = 1,\ldots, I$, $I \geq 1$. 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, а также ГОСТ Р 59331—2021 (В.2 приложения В), ГОСТ Р 59341—2021 (В.3 приложения В) и ГОСТ Р 59347—2021 (В.2 приложения В).

В.2.4 Оценка наличия недопустимого брака в поставляемых продукции и/или услугах

В.2.4.1 Общие положения

Вероятность наличия недопустимого брака в поставляемых продукции и/или услугах оценивают в виде вспомогательного показателя при проведении оценок интегрального риска нарушения реализации рассматриваемого процесса приобретения или поставки продукции и/или услуг с учетом требований по защите информации — см. В.4.2.

При реализации каждого процесса поставляемая продукция и/или услуги должны удовлетворять требованиям по качеству. Нарушение качества поставляемой продукции и/или услуги в системе — это угроза возможного ущерба. В общем случае под выполнением требований по качеству понимается поставка продукции и/или услуг без брака или с допустимым уровнем брака, оговоренным в договорных условиях. С точки зрения нарушения качества поставляемых продукции и/или услуг и тяжести возможного ущерба поставляемые продукция и/или услуги могут быть условно сгруппированы по J типам, $J \geq 1$. В общем случае для каждого типа количественные условия к отсутствию недопустимого брака формулируют в одном из двух видов:

- условие 1: количество единиц брака в j-й поставке продукции и/или услуг $H_{брака\,j}(T_{зад\,j})$ не должно превышать задаваемого уровня $H_{брака\,зад\,j}(T_{зад\,j}) \geq 0$, зависящего в общем случае от объема и сроков поставки $T_{зад\,j}$, ($j = 1,\ldots, J$). Для больших объемов поставки значение $H_{брака\,зад\,j}(T_{зад\,j})$ может быть по согласию заинтересованных сторон интерпретировано как количество допустимого брака в некоторых выборках;

- условие 2: допустимая вероятность брака $R_{брака\,j}(T_{зад\,j})$ в j-й поставке продукции и/или услуг не должна превышать $R_{брака\,зад\,j}(T_{зад\,j}) > 0$, т. е. задают максимально допустимый вероятностный уровень $R_{брака\,зад\,j}(T_{зад\,j})$ такой, чтобы соблюдалось ограничительное условие $R_{брака\,j}(T_{зад\,j}) \leq R_{брака\,зад\,j}(T_{зад\,j})$.

Неприемлемость нарушений задаваемых условий фиксируют в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение брака в процессе приобретения или поставки продукции и/или услуг для системы.

В.2.4.2 Метод оценки

При оценке риска вычисляют вероятность наличия брака при однократной и множественных поставках для разнородных продукции и/или услуг.

На основе применения статистических данных вероятность $R_{брака\,j}$ наличия брака при однократной поставке продукции и/или услуг j-го типа за задаваемое время $T_{зад\,j}$ вычисляют по формуле

$$R_{брака\,j}(T_{зад\,j}) = H_{наруш\,j}(T_{зад\,j}) / H_j(T_{зад\,j}), \qquad (В.8)$$

где $H_{наруш\,j}(T_{зад\,j})$ и $H_j(T_{зад\,j})$ — соответственно количество поставок с недопустимым браком и общее количество поставок продукции и/или услуг j-го типа за заданное время $T_{зад\,j}$ согласно статистическим данным.

Вероятность $R_{брака}(T_{зад})$ наличия брака по всему множеству продукции и/или услуг различных типов, реализуемых согласно статистическим данным в процессе приобретения с учетом множественности поставок, характеризуемых исходными данными по каждому из типов, вычисляют по формулам:

- для случая, когда учитывают все поставки (как с соблюдением, так и с нарушением условий по отсутствию недопустимого брака)

$$R_{брака}(T_{зад}) = 1 - \sum_{j=1}^{J} L_j [1 - R_{брака\,j}(T_{зад\,j})] / \sum_{j=1}^{J} L_j; \quad (В.9)$$

- для случая, когда учитывают лишь те поставки, для которых условия по отсутствию недопустимого брака были нарушены (именно они являются причиной возможных ущербов)

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

где $T_{зад}$ — задаваемое общее время поставки всего множества продукции и/или услуг различных типов, включающее в себя все частные значения $T_{зад\,j}$ с учетом их наложений;

L_j — количество учитываемых поставок продукции и/или услуг j-го типа при многократных поставках.

Индикаторная функция $Ind(\alpha) = Ind_{брака}(\alpha_j)$ позволяет учесть последствия, связанные с наличием брака в поставках — см. (В.1). Условие α_j, используемое в индикаторной функции, формируют из договорных документов путем анализа задаваемых условий 1 или 2 к отсутствию недопустимого брака при поставках — см. В.2.4.1.

Примечания

1 При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.9), (В.10) совпадают.

2 Практическая ценность расчетов применения формул (В.8)—(В.10) проявляется при общем количестве поставок $H_j(T_{зад\,j})$ за заданное время $T_{зад\,j}$ не менее 10 и количестве случаев поставок с недопустимым браком $H_{наруш\,j}(T_{зад\,j}) > 0$, $j = 1,\ldots, J$, $J \geq 1$. 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. В.3, а также ГОСТ Р 59331—2021 (В.2 приложения В), ГОСТ Р 59341—2021 (В.3 приложения В) и ГОСТ Р 59347—2021 (В.2 приложения В).

В.3 Прогнозирование рисков нарушения требований по защите информации

В.3.1 Общие положения

В.3.1.1 Прогнозирование рисков 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 любому из процессов приобретения или поставки продукции и/или услуг для системы 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 процессам и возможным условиям их реализации.

В.3.1.2 В моделях простой структуры под анализируемой системой понимают определенный выходной результат или действие, а также совокупность задействованных активов, к которым предъявлены требования и 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 рассматривается 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 усло-

вия 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 с возможным ущербом.

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

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

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

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение успешной реализации каждого из процессов приобретения или поставки продукции и/или услуг для системы.

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

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

В.3.1.6 При расчетах с использованием математических моделей для прогнозирования риска нарушения требований по защите информации и рекомендаций ГОСТ Р 59341—2021 (В.2, В.3 приложения В) осуществляют учет принимаемых 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 приобретения или поставки продукции и/или услуг для системы.

В.3.2 Исходные данные и расчетные показатели

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

σ — частота возникновения источников угроз нарушения требований по защите информации в процессе приобретения или поставки продукции и/или услуг для системы;

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

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

$T_{диаг}$ — 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:

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

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

Расчет показателей применительно к рассматриваемому процессу приобретения или поставки продукции и/или услуг для моделируемой системы простой и сложной структуры осуществляют по формулам ГОСТ Р 59341—2021 (В.2 приложения В).

Примечание — При необходимости могут быть использованы 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 каждого из рассматриваемых процессов приобретения или поставки продукции и/или услуг для системы 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 конкретного процесса, нарушения сроков поставки, наличия недопустимого брака в поставляемых продукции и/или услугах (см. В.2) и нарушения требований по защите информации (см. В.3) в сопоставлении с возможным ущербом.

В.4.2 Метод оценки

Вероятность $R_{интегр}$ ($T_{зад}$) нарушения надежности реализации рассматриваемого процесса приобретения или поставки продукции и/или услуг без учета требований по защите информации вычисляют по формулам:

- для случая, когда учитывают все действия и поставки (включая действия с нарушениями и отсутствием нарушений):

$$R_{интегр}(T_{зад}) = 1 - \{\sum_{k=1}^{K} W_k[1 - R_{действий\ k}(T_{зад\ k})] + \sum_{i=1}^{I} M_i[1 - R_{сш\ i}(T_{зад\ i})] + \sum_{j=1}^{J} L_j[1 - R_{брака\ j}(T_{зад\ j})]\} / (\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i + \sum_{j=1}^{J} L_j); \quad (В.11)$$

- для случая, когда учитывают лишь те поставки, для которых условия выполнения необходимых действий процесса и/или соблюдения сроков поставки и/или отсутствия недопустимого брака были нарушены (именно эти нарушения являются причиной возможных ущербов):

$$R_{интегр}(T_{зад}) = 1 - \{\sum_{k=1}^{K} W_k[1 - R_{действий\ k}(T_{зад\ k})]\, ind_{действий}(\alpha_k) + \sum_{i=1}^{I} M_i[1 - R_{сш\ i}(T_{зад\ i})] ind_{сш}(\alpha_i) + \sum_{j=1}^{J} L_j[1 - R_{брака\ j}(T_{зад\ j})] ind_{брака\ j}(\alpha_j)\} / (\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i + \sum_{j=1}^{J} L_j), \quad (В.12)$$

где $T_{зад}$ — задаваемое общее время прогноза, включающее в себя все частные значения $T_{зад\ k}$, $T_{зад\ i}$, $T_{зад\ j}$ с учетом их наложений — см. формулы (В.2)—(В.10).

Примечание — При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.11), (В.12) совпадают.

Интегральную вероятность нарушения реализации процесса приобретения или поставки продукции и/или услуг для системы с учетом требований по защите информации $R_{\text{интегр.уч}}(T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле

$$R_{\text{интегр.уч}}(T_{\text{зад}}) = 1 - [1 - R_{\text{интегр}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})]. \quad \text{(В.13)}$$

Здесь вероятность нарушения надежности реализации рассматриваемого процесса в течение периода прогноза без учета требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$ рассчитывают по формулам (В.11) или (В.12) в зависимости от целей системного анализа, а вероятность нарушения требований по защите информации в системе в течение периода прогноза $R_{\text{наруш}}(T_{\text{зад}})$ рассчитывают по рекомендациям В.3 для выбранной при проведении системного анализа структуры моделируемой системы.

Интегральный риск нарушения реализации рассматриваемого процесса приобретения или поставки продукции и/или услуг для системы с учетом требований по защите информации определяют путем сопоставления расчетной интегральной вероятности нарушения реализации процесса в течение периода прогноза, рассчитанной по формуле (В.13), с возможным ущербом за этот период.

Примечание — Примеры прогнозирования рисков и способы решения различных задач системного анализа см. в ГОСТ Р ИСО 11231, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение Г
(справочное)

Типовые допустимые значения показателей рисков для процессов приобретения и поставки

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

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

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

Типовые допустимые значения количественных показателей рисков для каждого из процессов приобретения или поставки продукции и/или услуг для системы отражены в таблице Г.1. При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые. В этом случае для задаваемых при моделировании условий имеет место гарантия надежной 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 приобретения или поставки продукции и/или услуг для системы	Не выше 0,05	Не выше 0,01
Интегральный риск нарушения реализации процесса приобретения продукции и/или услуг для системы с учетом требований по защите информации	Не выше 0,10	Не выше 0,05
Интегральный риск нарушения реализации процесса поставки продукции и/или услуг для системы с учетом требований по защите информации	Не выше 0,10	Не выше 0,05

Приложение Д
(справочное)

Примерный перечень методик системного анализа для процессов приобретения и поставки

Д.1 Методика прогнозирования риска нарушения требований по защите информации в процессе приобретения продукции и/или услуг для системы.

Д.2 Методика прогнозирования интегрального риска нарушения реализации процесса приобретения продукции и/или услуг для системы с учетом требований по защите информации.

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 приобретения продукции и/или услуг для системы с учетом требований по защите информации).

Д.4 Методики выявления явных и скрытых недостатков процесса приобретения продукции и/или услуг для системы с использованием прогнозирования рисков.

Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса приобретения продукции и/или услуг для системы 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 приобретения продукции и/или услуг для системы.

Д.7 Методика прогнозирования риска нарушения требований по защите информации в процессе поставки продукции и/или услуг для системы.

Д.8 Методика прогнозирования интегрального риска нарушения реализации процесса поставки продукции и/или услуг для системы с учетом требований по защите информации.

Д.9 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 в процессе поставки продукции и/или услуг для системы с учетом требований по защите информации).

Д.10 Методики выявления явных и скрытых недостатков процесса поставки продукции и/или услуг для системы с использованием прогнозирования рисков.

Д.11 Методики обоснования предупреждающих действий, направленных на достижение целей процесса поставки продукции и/или услуг для системы и противодействие угрозам нарушения требований по защите информации.

Д.12 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса поставки продукции и/или услуг для системы.

Примечания

1 Системной основой для создания методик служат положения разделов 5—7, методы и модели 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] Р 50.1.053—2005 Информационные технологии. Основные термины и определения в области технической защиты информации

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

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

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

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

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

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

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

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

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

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

Ключевые слова: актив, защита информации, модель, поставщик, приобретающая сторона, продукция, процесс поставки, процесс приобретения, риск, система, системная инженерия, управление, услуги

Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 29.04.2021. Подписано в печать 17.05.2021. 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