ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59346— 2021

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ СИСТЕМНЫХ ТРЕБОВАНИЙ

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФГУ ФИЦ ИУ РАН) и Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ ГНИИИ ПТЗИ ФСТЭК России)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 апреля 2021 г. № 332-ст

4 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

Введение

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

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

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

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

- для технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, 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 59347, ГОСТ Р 59348, ГОСТ Р 59349, ГОСТ Р 59350, ГОСТ Р 59351, ГОСТ Р 59352, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357. Для процесса определения системных требований — по настоящему стандарту.

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ СИСТЕМНЫХ ТРЕБОВАНИЙ

System engineering. Protection of information in system requirements definition process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа для процесса определения системных требований применительно к вопросам защиты информации в системах различного назначения.

Для практического применения в приложениях А—Ж приведены примеры перечней защищаемых активов и угроз, примерный состав моделей и методик для системного анализа в процессе определения системных требований, связанных с защитой информации, взаимосвязь показателей для оценки эффективности защиты информации в системе, методы, модели и примеры прогнозирования рисков нарушения безопасности информации в системе, методы определения допустимых значений рисков, методические указания по прогнозированию рисков и определению перечня существенных угроз безопасности информации.

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

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процесс определения системных требований, а также теми заинтересованными сторонами, которые уполномочены осуществлять контроль выполнения требований по защите информации в жизненном цикле систем — см. примеры систем в [1]—[14].

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

Издание официальное

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

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

ГОСТ 27.002 Надежность в технике. Термины и определения

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

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

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

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

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

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

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

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

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

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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

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

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

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

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

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

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

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

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

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

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

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

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

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

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

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

ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

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—2016 Системная и программная инженерия. Процессы жизненного цикла систем

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ 27.002, ГОСТ 34.003, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51897, ГОСТ Р 53114, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61508-4, а также следующие термины с соответствующими определениями:

3.1.1

актив (asset): Что-либо, что имеет ценность для организации.

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

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

3.1.2

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

[ГОСТ Р 51898—2002, пункт 3.9]

3.1.3

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]

3.1.4

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]

3.1.5

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]

3.1.6

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]

3.1.7

известная уязвимость: Уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений

[ГОСТ Р 56545—2015, пункт 3.7]

3.1.8 **надежность реализации процесса определения системных требований с учетом требований по защите информации:** Свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнить процесс в заданных условиях его реализации с соблюдением требований по защите информации.

3.1.9

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

[ГОСТ Р 50922—2006, статья 2.9.4]

3.1.10

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

[ГОСТ Р 50922—2006, статья 2.9.3]

3.1.11

правила описания уязвимости: Совокупность положений, регламентирующих структуру и содержание описания уязвимости

[ГОСТ Р 56545—2015, пункт 3.4]

3.1.12

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.13

система (system): 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]

3.1.14

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

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.1.15

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]

3.1.16

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

[ГОСТ Р 50922—2006, статья 2.6.1]

3.1.17

уязвимость: Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

[ГОСТ Р 56545—2015, пункт 3.3]

3.1.18

уязвимость нулевого дня: Уязвимость, которая становится известной до момента выпуска разработчиком компонента информационной системы соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

[ГОСТ Р 56545—2015, пункт 3.8]

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

3.1.20

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

[ГОСТ Р 50922—2006, статья 2.9.1]

3.2 В настоящем стандарте использованы следующие сокращения:

ЗИ — защита информации;

ИИ — искусственный интеллект;

ТЗ — техническое задание;

ПМП — полумарковский процесс;

СМО — система массового обслуживания;

СПМ — сеть Петри — Маркова.

4 Основные положения системной инженерии по защите информации в процессе определения системных требований

4.1 Общие положения

Организации используют процесс определения системных требований в рамках создания (модернизации, развития) и эксплуатации системы для преобразовании представления заинтересованных сторон о возможностях системы в требования, реализация которых удовлетворит эксплуатационные потребности пользователей системы и возможности разработчика, для обеспечения при этом эффективности защиты информации, а также для сохранения конфиденциальности сведений об активах системы и о самой системе. На стадии выведения системы из эксплуатации требования применения процесса направлено на защиту информации в части определения сроков и порядка выведения системы из эксплуатации, а также утилизации носителей защищаемой информации.

При планировании и реализации процесса определения системных требований осуществляют защиту информации, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должно быть обеспечено надежное выполнение процесса.

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

Определение выходных результатов процесса и типовых действий по защите информации осуществляют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р 51904, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, с учетом специфики системы и стандартов соответствующей отрасли (см., например ГОСТ 15.016, ГОСТ IEC 61508-3, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-7, [7]—[14]). Оценку различных рисков нарушения требований по защите информации осуществляют по настоящему стандарту с использованием рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 54124, ГОСТ Р 57102, ГОСТ Р 57272.1, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р 59355. При этом учитывают специфику системы и организации, применяющей процесс — см., например, [7]—[14].

4.2 Стадии и этапы жизненного цикла системы

Процесс определения системных требований может быть использован на любой стадии жизненного цикла системы. Стадии и этапы работ устанавливают в договорах, соглашениях и ТЗ с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, [1]—[6], [7]—[11], [14]. Процесс определения системных требований может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.3 Цели процесса и назначение мер защиты информации

4.3.1 Формирование целей процесса определения системных требований осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики системы. В общем случае цель процесса определения системных требований состоит в преобразовании ориентированного на пользователей представления заинтересованных сторон о возможностях системы в требования для такого технического предоставления решения, которое удовлетворит эксплуатационным потребностям пользователей и возможностям разработчика по реализации этих решений.

Применительно к стадии замысла, формирования требований, разработки концепции (концептуальных положений) и ТЗ цель процесса определения системных требований в части защиты информации состоит в пресечении возможности выявления существенной информации о самой системе и выбора мер и средств защиты информации (ЗИ), подлежащих использованию в системе для адекватного противодействия угрозам.

Примечание — Существенность информации рассматривается с точки зрения реализации угроз безопасности информации на текущей и последующих стадиях жизненного цикла системы.

Применительно к стадиям разработки, производства и поставки системы заказчику определение системных требований в части ЗИ должно быть направлено на предупреждение и пресечение возможностей несанкционированного внесения разработчиком недекларированных возможностей в программное и программно-аппаратное обеспечение системы и выявление существенной информации о самой системе (существенной с точки зрения реализации угроз безопасности информации при ее эксплуатации), а также на обоснование мер и средств ЗИ, подлежащих использованию на этих стадиях.

Применительно к стадии эксплуатации, включая сопровождение системы, требования в части ЗИ направлены на защиту информации о самой системе (в том числе о применяемых в ней мерах и средствах защиты информации) и об обрабатываемой в системе информации пользователей, сведений об организации и ее контрагентах, а также об иных системах, с которыми осуществляет взаимодействие рассматриваемая система.

Применительно к стадии выведения системы из эксплуатации требования в части ЗИ направлены на защиту информации, касающейся сроков и порядка выведения системы из эксплуатации, а также на утилизацию носителей защищаемой информации, исключающую возможность выявления ее содержания.

Применительно ко всем стадиям жизненного цикла в процессе определения системных требований проводится системный анализ различных процессов — см. ГОСТ Р 59349.

Использование процесса определения системных требований позволяет задать разработчику функциональные и эксплуатационные возможности, которыми система должна обладать для удовлетворения требований заинтересованных сторон, а также условия и меры ЗИ. Насколько допускают ограничения, системные требования не должны диктовать никакой конкретной реализации.

4.3.2 Меры ЗИ в процессе определения системных требований предназначены для конфиденциальности, целостности и доступности защищаемой информации, предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Определение мер ЗИ осуществляют по ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р МЭК 61508-7, [7]—[14] с учетом специфики системы и реализуемой стадии ее жизненного цикла.

4.4 Основные принципы системного анализа

При проведении системного анализа процесса определения системных требований 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. [7]—[14]). Все применяемые принципы подчинены принципу целенаправленности осуществляемых действий.

4.5 Основные усилия для обеспечения защиты информации

Основные усилия системной инженерии для обеспечения защиты информации в процессе определения системных требований сосредоточивают:

- 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, выявлении множества уязвимостей системного и прикладного программного обеспечения функционирования системы, которые могут быть использованы при реализации потенциальных угроз безопасности информации;

- определении и прогнозировании рисков, подлежащих системному анализу,

- проведении системного анализа для обоснования мер, направленных на противодействие угрозам и достижение целей процесса.

5 Общие требования системной инженерии по защите информации в процессе определения системных требований

5.1 Общие требования системной инженерии по защите информации устанавливают в ТЗ на выполнение работ. Эти требования и методы их выполнения детализируют в ТЗ на составную часть системы (в качестве составной части системы может выступать система защиты информации), в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Поскольку элементы процесса определения системных требований могут использоваться на этапах, предваряющих получение и утверждение ТЗ, соответствующие требования по защите информации, применимые к этому процессу, могут быть оговорены в рамках соответствующих договоров и соглашений. Содержание требований формируют при выполнении процесса с учетом нормативных правовых документов Российской Федерации (см., например [1]—[4], [7]—[14]), уязвимостей системы, преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов.

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

5.2 Требования системной инженерии по защите информации призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации процесса определения системных требований и поддержке при этом эффективности защиты информации.

К системным требованиям, связанным с ЗИ, в соответствии с общими требованиями системной инженерии относят:

- требования к описанию системы, касающиеся состава защищаемой информации, состава и места в системе ее программных и программно-аппаратных элементов, в которых обрабатывается такая информация, а также требования к описанию технических решений по взаимодействию рассматриваемой системы с другими системами;

- требования к составам выходных результатов, выполняемых действий и используемых при этом активов, подлежащих защите от угроз безопасности информации;

- требования к порядку выявления уязвимостей системы, угроз безопасности информации, реализуемых путем использования этих уязвимостей, а также требования к прогнозированию рисков реализации этих угроз на всех этапах жизненного цикла системы;

- требования по защите от преднамеренных и непреднамеренных угроз нарушения функционирования системы и/или ее программных и программно-аппаратных элементов;

- требования по защите от угроз утечки информации, содержащей сведения, не подлежащие распространению по требованиям заинтересованных сторон системы, а также по требованиям нормативных правовых актов государственных регуляторов в области ЗИ;

- требования к функциональным характеристикам системы защиты информации, обрабатываемой в системе и/или передаваемой по сетям общего пользования (в том числе по сети Интернет) или по выделенным каналам в сопряженные сети иных организаций, включая требования по обоснованию эффективных превентивных способов снижения рисков или их удержания в допустимых пределах;

- требования к нефункциональным характеристикам системы защиты (в том числе к мерам и способам обеспечения ее функционирования), включая требования по обоснованию эффективных превентивных организационных действий, направленных на снижение рисков или их удержание в допустимых пределах;

- требования, касающиеся проектных ограничений.

Примечание — В системах искусственного интеллекта (ИИ) возникает необходимость формирования требований, касающихся:

- гарантированного подтверждения достаточности автоматизированной анонимизации и деперсонификации конфиденциальной информации при предоставлении доступа разработчиков систем к обучающим наборам исходных данных, являющихся изначально конфиденциальными;

- учета возможности повышения уровня конфиденциальности данных в процессе их обработки в системе ИИ (по мере агрегирования, выявления скрытых зависимостей, восстановления изначально отсутствующей информации);

- регламентации процессов обеспечения конфиденциальности тестовых выборок исходных данных, используемых испытательными лабораториями при оценке соответствия прикладных систем ИИ, с сохранением прозрачности и подотчетности такой оценки.

5.3 Состав выходных результатов и выполняемых действий в процессе определения системных требований определяют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839 с учетом специфики системы.

5.4 Меры защиты информации и действия по защите информации должны охватывать активы, информация которых или о которых подлежит защите для получения выходных результатов и выполнения действий процесса определения системных требований.

Примечание — В состав активов могут быть включены активы, используемые для достижения целей процесса определения системных требований для иных систем, подсистем или средств, не вошедших в состав рассматриваемой системы, но охватываемых по требованиям заказчика — например, для привлекаемых средств контроля надежности.

5.5 Определение активов, информация которых или о которых подлежит защите, и формирование перечня потенциальных угроз и возможных сценариев возникновения и развития угроз для каждого из активов осуществляют по ГОСТ 34.602, ГОСТ IEC 61508-3, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58412 с учетом рекомендаций ГОСТ 15.016, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 59329, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6 и специфики системы (см., например, [7]—[14]).

Примеры перечней учитываемых активов и угроз в процессе определения системных требований приведены в приложениях А и Б.

5.6 Эффективность ЗИ при выполнении процесса определения системных требований оценивают по показателям, рассчитываемым на основе значений показателей рисков реализации угроз в условиях отсутствия мер защиты информации и прогнозируемого применения выбираемых мер защиты информации в зависимости от специфики системы и особенностей ее функционирования.

Системный анализ процесса осуществляют с использованием методов, моделей и методических указаний (см. приложения В, Г, Д, Е, Ж) с учетом рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1.

5.7 Для обоснования эффективных превентивных мер защиты, направленных на снижение различных рисков или их удержание в допустимых пределах, применяют системный анализ с использованием устанавливаемых специальных качественных и количественных показателей рисков и показателей эффективности ЗИ. Примерный состав методик системного анализа приведен в приложении В, типовая номенклатура показателей для оценки рисков и эффективности ЗИ в системе — в приложении Г, методы и модели для оценки рисков — в приложении Д, а методические указания по прогнозированию рисков и определению угроз безопасности информации — в приложении Ж.

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 и требования к специальным количественным показателям рисков в интересах системного анализа процесса определения системных требований определены в 6.2 и 6.3.

Характеристики мер ЗИ и исходные данные, обеспечивающие применение методов, моделей и методик, определяют на основе собираемых и накапливаемых сведений по реализованным угрозам безопасности информации, по применяемым или рекомендуемым к применению мерам, средствам и способам ЗИ в системах.

6 Специальные требования к количественным показателям

6.1 Общие положения

6.1.1 Применительно к защищаемым активам, действиям и выходным результатам процесса определения системных требований при необходимости устанавливают заданный уровень (класс) защищенности или категорию значимости (важности) системы. С учетом этого определяют возможные варианты мер защиты информации, с использованием которых может быть достигнут заданный уровень (класс) защищенности системы. Оценивают эффективность ЗИ на основе прогнозирования рисков в условиях возможных угроз. Осуществляют обоснование эффективных превентивных мер и действий по снижению рисков и/или их удержанию в допустимых пределах.

6.1.2 В общем случае основными выходными результатами процесса определения системных требований являются:

- установленный состав заинтересованных сторон системы в течение ее жизненного цикла;
- результаты анализа выявленных потребностей и требований заинтересованных сторон (см. ГОСТ Р 57193, ГОСТ Р 59344 и ГОСТ Р 59345);
- ТЗ на разработку системы и конкретные системные требования, отражающие потребности и требования заинтересованных сторон;
- отчеты о прослеживаемости сформулированных системных требований относительно удовлетворения потребностей и требований заинтересованных сторон на всех стадиях жизненного цикла системы;
- характеристики и условия использования возможностей системы для ЗИ, критические показатели влияния предлагаемых мер защиты информации на функционирование системы и снижение рисков реализации угроз или их удержание в допустимых пределах;
- ограничения со стороны системных требований для принимаемых системных решений;
- системные требования к обеспечивающим системам, которые предполагается использовать в жизненном цикле рассматриваемой системы;
- достигнутые соглашения с заинтересованными сторонами о том, что их потребности и требования правильно отражены в сформулированных системных требованиях;
- функциональное описание системы, включая ее границы и взаимодействия;
- материалы в отчеты об обследовании объектов системы, проведении необходимых научно-исследовательских работ.

6.1.3 Для получения выходных результатов процесса определения системных требований в общем случае выполняют следующие основные действия:

- определение заинтересованных сторон системы в течение ее жизненного цикла;
- определение и анализ потребностей и требований заинтересованных сторон, представляющих начальные неформальные посылки для технических решений (замысел новой системы, модернизация или развитие существующей системы);
- определение контекста использования рассматриваемой системы, требований и порядка взаимодействия с другими системами, необходимыми для обеспечения установленных потребностей и требований заинтересованных сторон;
- разработку концепции функционирования (эксплуатации) системы и других концепций жизненного цикла системы, включая определение сценариев функционирования и порядка взаимодействия между пользователями и системой;
- преобразование потребностей и требований заинтересованных сторон в конкретные системные требования, включая:
- требования к критичным характеристикам, таким как уровень (класс) защищенности или категория значимости системы, показатели защищенности системы от возможных угроз безопасности информации, показатели защищенности окружающей среды и здоровья персонала, пользователей и окружающего населения (при необходимости),
- требования, связанные со сценариями, взаимодействиями, ограничениями и критичными характеристиками качества, безопасности и эффективности системы в ее жизненном цикле,
- требования по ограничению принимаемых системных решений, вытекающие из существующих соглашений, управленческих и технических возможностей;
- системный анализ потребностей и требований заинтересованных сторон, включая обеспечение обратной связи с заинтересованными сторонами для получения гарантии того, что их потребности, требования и ожидания правильно интерпретированы и выражены в системных требованиях;

- поддержание основных информационных активов, создаваемых в рамках процесса определения системных требований;

- формирование ТЗ на выполнение определенных работ, необходимых для последующей реализации системных требований.

6.1.4 Текущие данные, накапливаемая и собираемая статистика, связанные с нарушениями требований по ЗИ и по защите системы от угроз нарушения ее функционирования, являются основой для принятия решений по факту наступления событий и источником исходных данных для прогнозирования рисков. Риски оценивают объективными вероятностными показателями, вычисляемыми путем моделирования (см. приложения Г, Е) или с использованием экспертного балльного метода (см. приложение Д) с учетом возможного ущерба.

6.2 Требования к составу показателей

Показатели должны обеспечивать проведение:

- прогнозирования рисков нарушения надежности реализации процесса определения системных требований;

- прогнозирования рисков реализации преднамеренных угроз безопасности информации в системе с учетом выполняемых мер ЗИ;

- оценки эффективности защиты информации в системе и о системе в зависимости от установленного для нее уровня (класса) защищенности или категории значимости применительно к каждой стадии жизненного цикла и в целом за весь жизненный цикл системы.

Показатели рисков реализации возможных угроз используют для оценки влияния предлагаемых мер защиты на снижение рисков или их удержание в допустимых пределах.

Показатели эффективности ЗИ применяют:

- для формирования представления о текущих и потенциальных проблемах или о возможных причинах, обусловливающих возможность реализации угроз безопасности информации;

- для сравнения эффективности применяемых и/или возможных мер в действующей системе защиты информации, выбора и оптимизации состава применяемых мер и действий по защите информации.

При оценке эффективности ЗИ дополнительно могут быть использованы вспомогательные статистические данные об инцидентах нарушения безопасности и последствиях в интересах уточнения их потенциального влияния на эффективность.

6.3 Требования к количественным показателям прогнозируемых рисков

6.3.1 Для прогнозирования рисков в процессе определения системных требований используют следующие количественные показатели:

- частные показатели риска реализации угроз безопасности информации в условиях отсутствия мер ЗИ, предлагаемых к использованию в процессе определения системных требований;

- частные показатели риска реализации угроз безопасности информации в случае применения мер ЗИ, предлагаемых к использованию в процессе определения системных требований (т. е. показатели остаточного риска при нарушении требований по ЗИ);

- интегральный риск нарушения функционирования системы и утечки защищаемой информации при применении мер ЗИ (предлагаемых к использованию в процессе определения системных требований);

- показатель риска нарушения надежности реализации процесса определения системных требований в части ЗИ.

6.3.2 В качестве частных показателей риска реализации угроз безопасности информации используют вероятности реализации угроз в системе в условиях выполнения сформулированных системных требований. При их расчетах должны быть учтены защищаемые активы, последствия, которые могут иметь место при реализации угроз, и выходные результаты в части защиты от этих угроз на каждой стадии и в течение всего жизненного цикла системы в соответствии с предъявляемыми системными требованиями.

6.3.3 Интегральный риск нарушения функционирования системы и утечки защищаемой информации характеризуют соответствующей вероятностью нарушения установленных требований по ЗИ (т. е. вероятностью реализации совокупности угроз безопасности информации или на одной из стадий жизненного цикла системы, или на некоторой выбранной совокупности стадий, или на протяжении всего жизненного цикла) в сопоставлении с возможным ущербом.

6.3.4 В качестве показателя риска нарушения надежности реализации процесса определения системных требований в части ЗИ используют вероятность нарушения надежности реализации этого процесса, которая является функцией частных показателей рисков реализации угроз безопасности информации в системе.

6.3.5 Для оценки эффективности ЗИ и надежности реализации процесса определения системных требований используют:

- разностные показатели, представляющие собой разность между достигаемым значением вероятности реализации угрозы нарушения функционирования системы или утечки конфиденциальной информации и предельно допустимым значением этой вероятности;
- относительные показатели, представляющие собой отношение предельно допустимого значения вероятности реализации угрозы (например, выхода системы из строя, нарушения ее функционирования или утечки конфиденциальной информации) к достигаемому ее значению;
- разностно-относительные показатели, представляющие собой отношение разности между достигаемым значением расчетной вероятности (например, выхода из строя системы, нарушения ее функционирования в результате реализации угроз безопасности информации или утечки конфиденциальной информации) и предельно допустимым значением этой вероятности к достигаемому значению расчетной вероятности.

6.3.6 Номенклатура и взаимосвязь количественных показателей для оценки рисков реализации угроз безопасности информации, рисков нарушения надежности реализации процесса определения системных требований и оценки эффективности ЗИ приведена в приложении Г. В случае, когда статистических данных для оценки возможных ущербов и рисков реализации угроз недостаточно или невозможен учет некоторых существенных факторов аналитическими методами, применяют экспертные методы (см. приложение Д).

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессу определения системных требований):

- временные характеристики реализации угроз безопасности информации в системе, в том числе временные характеристики преодоления мер и средств ЗИ, используемых в системе;
- статистические данные о состоянии параметров системы защиты информации (привязанные к временам изменения состояний), дающие представление о реакции исполнительных механизмов системы защиты на процессы реализации угроз;
- статистические данные о системах-аналогах, характеризующие не только данные о нарушениях их функционирования, но и о событиях, связанных с утечкой защищаемой информации, несанкционированными или непреднамеренными воздействиями на защищаемую информацию (привязанные к временам наступления событий, характеризующих нарушения и предпосылки к нарушениям требований по ЗИ);
- текущие и статистические данные результатов технического диагностирования системы защиты информации, а также данные технического контроля выполнения установленных требований по ЗИ;
- наличие и готовность персонала системы защиты информации, данные об ошибках персонала (привязанные к временам наступления событий, характеризующих нарушения и предпосылки к нарушениям требований по ЗИ), а также о последствиях этих ошибок для рассматриваемой системы или для системы, выбранной в качестве аналога при расчетах количественных показателей;
- данные, получаемые по результатам моделирования угроз, и сведения, позволяющие определить перечень потенциальных угроз и возможные сценарии их возникновения и развития для каждого из защищаемых активов.

Типовые исходные данные для моделирования приведены в приложениях Г, Д, Е, Ж.

7 Требования к системному анализу

7.1 Общие положения

7.1.1 Требования к системному анализу процесса определения системных требований включают:

- требования к прогнозированию рисков и обоснованию допустимых рисков;
- требования к выявлению уязвимостей системы (в том числе ее аппаратного, системного и прикладного программного обеспечения) и угроз безопасности информации, реализуемых с использованием уязвимостей;

- требования к поддержке принятия решений в жизненном цикле системы.

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

7.1.2 При обосновании и формулировании требований к системному анализу дополнительно руководствуются требованиями 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 51275, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57272.1, ГОСТ Р 58412, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы.

7.2 Требования к прогнозированию рисков

7.2.1 Для прогнозирования рисков нарушения требований по ЗИ в процессе определения системных требований должны быть:

- определены перечни выходных результатов и составных действий процесса, а для каждого из них — используемые активы (см. приложение А) и потенциальные угрозы безопасности информации (см. приложения Б и Ж);
- определен требуемый класс (уровень) защищенности системы или ее категория значимости при наличии официальных требований по категорированию (или классификации по уровням, классам защищенности) таких систем;
- определены количественные показатели прогнозируемых рисков реализации возможных угроз безопасности информации в системе;
- выбраны, адаптированы или разработаны модели и методы для прогнозирования рисков (см. приложение Д);
- собраны исходные данные в интересах применения моделей и методик для прогнозирования рисков;
- предусмотрен механизм использования результатов прогнозирования рисков.

Примечание — Требуемые классы (уровни) защищенности и категории значимости устанавливаются постановлениями Правительства Российской Федерации, действующими нормативными документами государственных регуляторов в области ЗИ в интересах реализации дифференцированного подхода к защите информации в системах.

7.2.2 Прогнозирование рисков используют для формального решения задач, связанных с ранним распознаванием и оценкой развития предпосылок к нарушению требований по ЗИ, обоснованием эффективных превентивных мер по снижению рисков или их удержанию в допустимых пределах, выявлением возможных угроз, поддержкой принятия решений по выполнению процесса определения системных требований.

В зависимости от содержания решаемых задач ЗИ прогнозируемый риск связывают с заранее определенным периодом прогноза (например, на месяц, год, несколько лет вперед), при этом учитывают развитие способов реализации угроз, совершенствование мер и средств ЗИ, которые могут быть применены в системе.

Примечание — Период прогноза может быть связан, например, с возникновением новых уязвимостей системного и прикладного программного обеспечения и разработкой специальных программ для их эксплуатации («эксплойтов»), с динамикой разработки новых вредоносных программ для реализации угроз.

7.3 Требования к обоснованию допустимых рисков

7.3.1 Допустимые риски нарушения требований по ЗИ в процессе определения системных требований выступают в качестве характеристики количественных норм эффективности ЗИ. Эти допустимые риски определяют при формировании системных требований для каждой стадии жизненного цикла и для всего жизненного цикла системы и задают во внутренних документах организации. Допустимые риски могут быть установлены в договорах, соглашениях и ТЗ с учетом специфики системы.

7.3.2 Количественное обоснование допустимых рисков осуществляют:

- применительно к рискам нарушения функционирования системы в результате реализации угроз безопасности информации;
- применительно к рискам утечки информации о системе или информации, обрабатываемой в системе и не подлежащей распространению по требованиям заказчика, разработчика или поставщика системы, а также по требованиям нормативных правовых актов федеральных органов исполнительной власти — государственных регуляторов в области ЗИ;

- применительно к риску нарушения надежности реализации процесса определения системных требований.

Допустимые риски нарушения функционирования системы устанавливают с учетом требуемого класса (уровня) защищенности системы или категории ее значимости, если она отнесена к значимым объектам критической информационной инфраструктуры (см. [6], [14]). При этом с учетом возможного ущерба допустимый риск определяют как допустимое значение вероятности того, что может быть реализована хотя бы одна из возможных существенных угроз, направленных на нарушение функционирования системы. Пример определения допустимого риска реализации угроз нарушения функционирования системы приведен в приложении Е.

Допустимые риски утечки информации о системе или информации, обрабатываемой в системе и не подлежащей распространению по требованиям заказчика, разработчика или поставщика системы, а также по требованиям нормативных правовых актов государственных регуляторов в области ЗИ, могут быть определены, например, на основе прецедентного принципа или путем экспертного перевода качественных оценок допустимого риска в количественные значения (см. приложение Д).

При использовании прецедентного принципа (см. также ГОСТ Р 59349):

- выявляют уязвимости системного и прикладного программного обеспечения, которые могут быть использованы для несанкционированного проникновения в операционную среду (получения доступа к командам операционной системы), в том числе уязвимости «нулевого дня», а также, по возможности, новых (неизвестных ранее) уязвимостей;

- выявляют прецеденты эксплуатации выявленных уязвимостей, наличие специальных программ, предназначенных для эксплуатации выявленных уязвимостей («эксплойтов»), и способы реализации угроз;

- определяют внешние (при наличии подключения к сетям общего пользования) и внутренние источники угроз безопасности информации, в том числе вредоносные программы, которые могут быть использованы для проникновения в операционную среду системы и воздействия (копирования, уничтожения, блокирования, несанкционированного запуска исполняемых файлов приложений) на защищаемую информацию, выявляют возможные способы инфицирования системы на стадии ее функционирования;

- формируют перечень реализованных угроз или попытки реализации которых имели место в выявленных инцидентах нарушения безопасности, выявляют возможные способы реализации угроз и оценивают вероятностно-временные характеристики реализации угроз в выявленных инцидентах.

Примечание — При этом может быть использован Банк данных угроз безопасности информации, сопровождаемый соответствующим государственным регулятором, в котором содержатся сведения об уязвимостях применяемых в России программных продуктов как отечественных, так и зарубежных разработчиков.

Расчетные значения рисков реализации угроз утечки информации на задаваемый период прогноза, свойственные состоявшимся нарушениям, связанным с проникновением в операционную среду рассматриваемой системы и/или систем, выбранных в качестве аналога, определяют как недопустимые, а меньшие по сравнению с минимальным недопустимым значением, при которых не было нарушений требований по ЗИ, определяют как допустимые. Для этого периода прогноза во множестве расчетных значений допустимых рисков выбирают максимальное значение. Поскольку это значение допустимого риска отвечает задаваемым условиям функционирования системы и априори является приемлемым для заинтересованных сторон, его признают в качестве допустимого по факту прецедента. Это значение допустимого риска устанавливают в качестве нормы эффективности ЗИ по прецедентному принципу и используют для формального решения задач системной инженерии.

Примечание — При отсутствии собственной статистики для рассматриваемой системы допускается использование статистики для похожих систем, в том числе из разных областей приложения. Применительно к системному анализу рисков такие системы рассматриваются как аналоги.

Экспертный метод преобразования качественных суждений о допустимом риске реализации угроз в количественные значения допустимой вероятности реализации угрозы основывается на теории нечетких суждений. Его применяют в том случае, когда статистика нарушений по возможным угрозам безопасности информации в рассматриваемой системе (и существующих аналогах системы) крайне мала, т. е. не позволяет сформировать аргументированные исходные данные для моделирования, или отсутствует вообще. При этом применяют балльный метод — см., например ГОСТ Р ИСО/МЭК 27005.

Примечание — Отсутствие достаточной статистики на практике является следствием возрастающей интенсивности возникновения новых уязвимостей (например, в системном и прикладном программном обеспечении систем и преимущественного их применения или применения уязвимостей «нулевого дня»), а также широкомасштабной разработкой новых способов реализации угроз, свойственным условиям возможных несанкционированных информационно-технических воздействий на систему (см. также ГОСТ Р 59342, ГОСТ Р 59355).

Примеры расчета допустимого риска реализации угроз и риска нарушения надежности реализации процесса определения системных требований в части ЗИ приведены в приложении Е.

7.4 Требования к выявлению угроз безопасности информации

7.4.1 Формирование перечня существенных угроз в процессе определения системных требований выполняют по результатам оценки рисков реализации возможных угроз.

При использовании прецедентного принципа для возможных анализируемых угроз должны рассматриваться одинаково защищаемые активы в разных системах-аналогах. Те угрозы, для которых значение прогнозируемого риска превышает средний уровень среди сравниваемых вариантов, отмечают как потенциальные угрозы. Из этих угроз путем проведения дополнительного системного анализа выбирают те, для которых риск реализации превышает допустимый, эти угрозы характеризуют как существенные. При изменении условий потенциальные угрозы могут переходить в разряд существенных угроз.

Если по результатам анализа прецедентов выявлено, что в ходе реализации угроз воздействию подвергались разные активы и/или применялись разные меры ЗИ, то проводят дополнительный системный анализ возможности перенесения результатов анализа прецедентов на рассматриваемую систему и приемлемости характеристики данных угроз как существенных для системы. Отнесение угрозы к существенной в этом случае считается обоснованным, если:

- содержание информации в активе или об активе не влияет на процесс реализации угрозы;
- можно сопоставить наборы мер и средств защиты, применяемых в системах-аналогах, для которых выявлены прецеденты нарушения безопасности информации, и результаты такого сопоставления учтены в сформированном значении допустимого риска реализации конкретной угрозы в рассматриваемой системе;
- несмотря на различия в составе конкретного множества действий в реализации угрозы замена этих действий на реализуемые в рассматриваемой системе несущественно скажется на риске реализации угрозы.

Таким образом угроза относится к существенной, если расчетный риск ее реализации превышает установленное значение допустимого риска. Непревышение допустимого риска характеризует отсутствие существенной угрозы в течение заданного периода прогноза. На практике эти результаты расчетов интерпретируют так: подобными угрозами, для которых риск удерживается в допустимых пределах, возможно пренебречь.

Примечание — Ситуации, когда применительно к рассматриваемой системе все расчетные риски не превышают установленных допустимых рисков, означают несущественность или отсутствие реальных угроз в течение всего периода прогноза. Если же все расчетные риски превышают максимально допустимые, это означает полную неприемлемость рассматриваемой системы с точки зрения обеспечения ЗИ для установленных допустимых рисков.

7.4.2 Если прецедентов по реализации рассматриваемых угроз нет или статистических данных недостаточно, то для выявления угроз используют моделирование. Краткая характеристика методов и моделей, которые могут быть использованы, приведена в приложении Д, см. также ГОСТ Р 59339, ГОСТ Р 59349.

Примечание — К примеру, при моделировании процессов реализации угроз, направленных на нарушение функционирования автоматизированной системы, определяют тип и версию операционной системы, состав и местонахождение системных файлов и их дескрипторных таблиц, нарушение которых может привести к сбою в функционировании системы, тип и версию системы управления базами данных, состав и местонахождение исполняемых файлов прикладных программ, а также выявляют известные неустраненные уязвимости системного программного обеспечения, использование которых возможно при реализации угроз. Так, при моделировании реализации угроз, направленных на нарушение конфиденциальности, целостности и/или доступности пользовательской информации, определяют состав файлов пользовательской информации и их местонахождение на логических дисках, в директориях и каталогах файловой системы, записи об этих файлах в дескрипторных таблицах, типы и версии прикладных программ, состав записей в электронных базах данных, содержащих сведения, не подлежащие распространению по требованиям заказчика, разработчика или поставщика системы в течение заданного времени (например, времени сохранения коммерческой ценности информации, времени устаревания данных, длительности стадии жизненного цикла системы).

7.4.3 Для моделирования определяют перечень возможных угроз, формируют функциональные, а затем математические модели реализации угроз и оценивают вероятности реализации угроз за задаваемый период времени.

7.4.4 По результатам моделирования оценивают вероятность реализации каждой угрозы и ее значение сравнивают с допустимым. Если вероятность реализации угрозы выше допустимой, то угрозу относят к существенной и для защиты от этой угрозы должны приниматься соответствующие меры.

Примечание — Для определения перечня существенных угроз могут быть использованы экспертные методы (см. 6.3.6). Пример экспертного определения перечня существенных угроз с использованием балльного метода приведен в приложении Д.

7.5 Требования к поддержке принятия решений

7.5.1 Прогнозирование рисков, обоснование допустимых рисков, обоснование эффективных превентивных мер по снижению рисков или их удержанию в допустимых пределах, выявление угроз в процессе определения системных требований осуществляют для поддержки принятия решений:

- по обеспечению выполнения процесса определения системных требований и норм эффективности ЗИ;
- по обоснованию мер, направленных на достижение целей процесса, противодействие угрозам и определение сбалансированных решений по ЗИ как на отдельных стадиях, так и на протяжении всего жизненного цикла системы;
- по обоснованию предложений по совершенствованию и развитию системы защиты информации.

Определяемые при этом допустимые риски играют роль ограничений для аналитического обоснования принимаемых решений.

7.5.2 Поддержка принятия решений по обеспечению выполнения процесса определения системных требований основана на прогнозировании различных рисков — см. 6.3 и приложения В, Д. При этом должна быть обеспечена поддержка принятия решений по прогнозированию риска нарушения требований по ЗИ, обоснования допустимых рисков — см. 7.2, 7.3. Это позволит определить нормы эффективности ЗИ и решить задачи, связанные с выполнением этих норм — см. 7.4.

7.5.3 Поддержка принятия решений по обоснованию мер, направленных на достижение целей процесса определения системных требований и противодействие угрозам, основана на предварительных прогнозах рисков реализации угроз в условиях применения возможных мер ЗИ. Состав возможных мер ЗИ определяется заранее в интересах снижения рисков нарушения требований по защите информации и/или их удержанию в допустимых пределах, а также в интересах восстановления приемлемых условий выполнения процесса определения системных требований в случае выявления предпосылок к нарушениям — см. 4.2.

Причины наступления событий, связанных с выявленными предпосылками к нарушению требований по ЗИ, фактами реализации угроз и произошедшими нарушениями установленных требований, регистрируют для недопущения подобных повторений и/или уточнения мер ЗИ, обеспечения приемлемых условий выполнения процесса определения системных требований и наполнения базы знаний.

7.5.4 Поддержка принятия решений по определению сбалансированных решений по ЗИ основана на системном анализе значений расчетных показателей рисков при сроках прогноза от месяца до одного года или нескольких лет.

При недопустимых значениях прогнозируемых рисков и/или при наступлении реальных нарушений в процессе определения системных требований должны быть выявлены их причины и определены меры для целенаправленного восстановления условий выполнения процесса на уровне рисков, не превышающих допустимые.

7.5.5 Поддержка принятия решений по обоснованию предложений, связанных с совершенствованием и развитием системы защиты информации основана на изучении результатов системного анализа рисков при сроке прогноза от нескольких месяцев до нескольких лет. Реализация этих предложений должна быть учтена в долгосрочных планах организации.

Примечания

1 Для обоснования мер, направленных на достижение целей процесса, противодействие угрозам, обоснование сбалансированных решений по ЗИ, обоснование предложений по совершенствованию и развитию системы защиты информации используют методы, модели и методики системного анализа, оценки риска и методические указания по прогнозированию рисков — см. приложения В—Ж, а также ГОСТ Р 59349.

2 Примеры решения задач системного анализа в приложении к различным системным 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 59347, ГОСТ Р 59356.

Приложение А
(справочное)

Пример перечня защищаемых активов

Перечень защищаемых активов в процессе определения системных требований может включать (в части, свойственной этому процессу):

- выходные результаты процесса — по 6.1.2;
- активы государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, значимых объектов критической информационной инфраструктуры Российской Федерации — см. [7]—[14];
- договоры и соглашения на проведение работ по созданию (модернизации, развитию) системы, выведению системы из эксплуатации;
- конструкторскую и технологическую документацию — по ГОСТ 2.051, ГОСТ 2.102, ГОСТ 3.1001;
- эксплуатационную и ремонтную документацию — по ГОСТ 2.602, ГОСТ Р 2.601;
- документацию на автоматизированные системы — по ГОСТ 34.201;
- программную документацию — по ГОСТ 19.101;
- документацию при выполнении научно-исследовательских работ — по ГОСТ 7.32, ГОСТ 15.101;
- программное обеспечение создаваемой и применяемой системы и средства его разработки и сопровождения;
- текстовые, графические, аудио- и видеофайлы, содержащие информацию, не подлежащую распространению по требованиям заказчика, разработчика или поставщика, в т. ч. файлы, содержащие результаты аудита системы;
- служебную информацию о деятельности предприятия, организации или отдельных должностных лиц, информацию о бухгалтерской и финансовой отчетности;
- содержание требований по ЗИ, предъявляемых в процессе определения системных требований;
- состав и характеристики мер и средств ЗИ, подлежащих применению в системе;
- персональные данные, базу данных и базу знаний, систему хранения архивов в части, связанной с процессом определения системных требований;
- систему передачи данных и облачные данные организации, связанные с процессом определения системных требований;
- выходные результаты иных процессов в жизненном цикле системы с учетом ее специфики.

Приложение Б
(справочное)

Пример перечня угроз

В процессе определения системных требований учитывают угрозы безопасности информации (в части, свойственной этому процессу), которые могут иметь место на всех стадиях жизненного цикла системы.

На стадии замысла, формирования требований, разработки концепции (концептуальных положений) построения системы и ТЗ перечень угроз может включать угрозы:

- проникновения в операционные среды автоматизированных систем разработчика и несанкционированного копирования информации, содержащей сведения, не подлежащие распространению;
- перехвата информации, передаваемой по сетям общего пользования и содержащей сведения о системе, не подлежащие распространению.

На стадиях разработки, производства и поставки системы возможна реализация угроз:

- проникновения в операционные среды автоматизированных систем разработчика или поставщика и несанкционированного копирования информации, содержащей сведения, не подлежащие распространению, в том числе сведения о мерах и средствах ЗИ, подлежащих применению в системе;
- внедрения в систему вредоносных программ, обеспечивающих возможности проникновения в операционную среду системы и нарушения процесса ее функционирования, в том числе путем изменения критически важных настроек системы, копирования пользовательской информации и передачи ее по сети общего пользования;
- перехвата информации, передаваемой по сетям общего пользования и содержащей сведения о системе, не подлежащие распространению.

На стадии эксплуатации системы, в том числе на стадии сопровождения (технического обслуживания), возможна реализация угроз:

- проникновения в операционную среду системы из сетей общего пользования и несанкционированного копирования информации, содержащей сведения, не подлежащие распространению, и изменения настроек, приводящего к нарушению нормального функционирования системы или выводу ее из строя;
- внедрения в систему вредоносных программ, обеспечивающих возможности нарушения процесса ее функционирования, в том числе путем блокирования команд, изменения критически важных настроек, подмены измерительной информации, передачи специально сформированных команд управления системой, а также возможности копирования пользовательской информации, создаваемой в процессе функционирования системы и передачи ее по сети общего пользования;
- непреднамеренного изменения, уничтожения, блокирования легитимными пользователями измерительной, командной или иной информации, существенной для правильного функционирования системы или ее средств ЗИ;
- непреднамеренной или преднамеренной, в том числе скрытной, передачи информации о системе, персональных данных, информации, составляющей коммерческую тайну, и иной информации, не подлежащей распространению.

На стадии выведения системы из эксплуатации возможна реализации угроз:

- несанкционированного копирования информации, сохранившейся на утилизируемых носителях информации и не подлежащей распространению;
- перехвата информации, передаваемой по сети общего пользования и касающейся факта и сроков вывода системы из эксплуатации, персональных данных, информации, составляющей коммерческую тайну, и иной информации, не подлежащей распространению.

Приложение В
(справочное)

Примерный состав моделей и методик для системного анализа в процессе определения системных требований, связанных с защитой информации

В.1 Типовые модели и методики охватывают следующие аспекты системного анализа в процессе определения системных требований:

- оценку рисков нарушения надежности реализации процесса определения системных требований;
- оценку рисков реализации угроз безопасности информации применительно к этапам жизненного цикла системы и интегрального риска нарушения надежности реализации процесса определения системных требований с учетом требований по ЗИ;
- выявление уязвимостей общесистемного и прикладного программного обеспечения функционирования системы (для автоматизированных систем);
- обоснование допустимых рисков нарушения требований по ЗИ и реализации угроз на отдельных стадиях и в процессе всего жизненного цикла системы;
- выявление существенных угроз безопасности информации в жизненном цикле системы;
- поддержку принятия решений по обоснованию эффективных мер ЗИ.

В сводном виде примерный состав моделей и методик для системного анализа в процессе определения системных требований, связанных с защитой информации, приведен на рисунке В.1.

В.2 Оценка рисков нарушения надежности реализации процесса определения системных требований охватывает риски нарушения функционирования программного и аппаратного обеспечения системы и риски реализации угроз безопасности информации на отдельных стадиях и в течение всего жизненного цикла системы.

Модель для оценки показателей рисков нарушения надежности реализации процесса определения системных требований описана в Д.1.

Примечание — При выявлении уязвимостей системного и прикладного программного обеспечения системы проводится анализ сведений, содержащихся в Банке данных угроз безопасности информации, сопровождаемого государственным регулятором.

В.3 Риски реализации угроз безопасности информации в системе возникают в результате:

- преднамеренных действий, направленных на нарушение функционирования системы или на выявление информации о системе, прикладных программах и данных, реализуемых внешними источниками угрозы (например, физическими лицами или программными средствами, функционирующими или действующими из-за пределов контролируемой территории);
- действий или функционирования внутренних источников угроз (например, преднамеренных и непреднамеренных действий сотрудников организации в пределах контролируемой территории, направленных на нарушение установленных требований по безопасности функционирования системы и обрабатываемой в ней информации);
- активизации установленных и функционирующих в системе программных, программно-аппаратных закладок, внедренных в нее вредоносных программ, инициация которых приводит к нарушению функционирования системы или к несанкционированным действиям относительно защищаемой информации.

Риски реализации угроз оценивают с использованием количественных показателей, методов и моделей в соответствии с методическими указаниями, изложенными в приложениях Г, Д, Ж. В системной инженерии результаты количественной оценки рисков используют в процессе управления рисками и при решении задач системного анализа (см. ГОСТ Р 59339, ГОСТ Р 59349).

В.4 Обоснование допустимых рисков реализации угроз безопасности информации проводят отдельно для угроз, направленных на нарушение функционирования системы, и угроз утечки информации, не подлежащей распространению по требованиям нормативных правовых актов федеральных органов исполнительной власти — государственных регуляторов в области ЗИ, а также по требованиям заказчика, разработчика и/или поставщика системы.

Примечание — Допустимые риски реализации угроз безопасности информации могут определять, например, на основе прецедентного принципа, на основе вводимой шкалы экспертного перевода качественных оценок допустимых возможностей реализации угроз в количественные значения допустимого риска такой реализации (см. приложение Д), с использованием методов расчета, изложенных в приложении Е и рекомендаций ГОСТ Р 59339, ГОСТ Р 59349.

В.5 Для выявления существенных угроз безопасности информации на стадиях и в процессе всего жизненного цикла системы используют результаты оценки рисков в сравнении с допустимыми значениями (см. приложение Ж).

В.6 Поддержка принятия решений по обоснованию эффективных мер ЗИ, направленных на достижение целей процесса и противодействие угрозам, основана на количественных оценках степени снижения рисков в условиях применения предлагаемых мер и средств ЗИ. Оценка снижения рисков проводится в соответствии с комплексом аналитических или имитационных моделей, характеристика которых приведена в приложении Д.

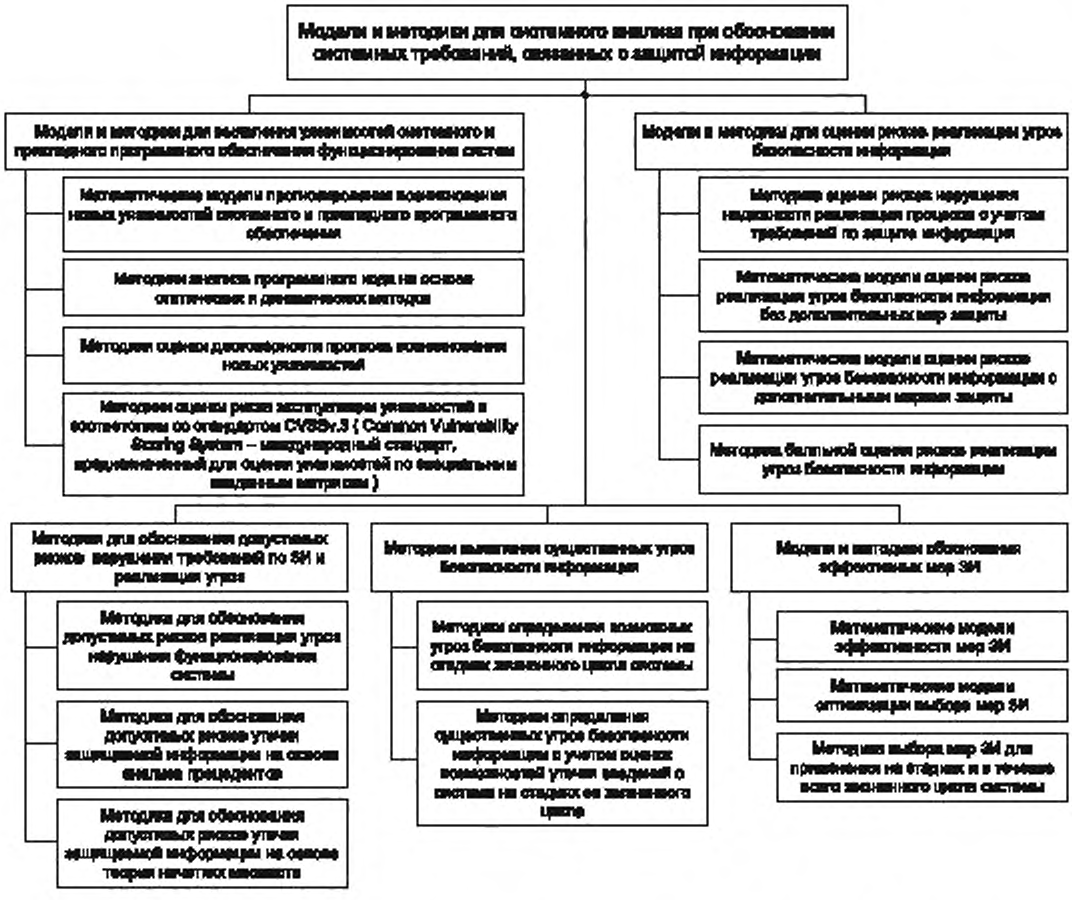


Рисунок В.1 — Примерный состав моделей и методик для системного анализа в процессе определения системных требований, связанных с защитой информации

Приложение Г
(справочное)

Взаимосвязь показателей для оценки эффективности защиты информации

Г.1 Показатели для оценки рисков применяют в процессе определения системных требований при обосновании необходимости ЗИ в системе на всех стадиях ее жизненного цикла, определении перечня существенных угроз безопасности информации, выборе мер и средств защиты и построении системы защиты информации, а также при обосновании предложений по совершенствованию и развитию системы защиты информации при модернизации и развитии системы.

Г.2 Показатели для оценки рисков включают:

- показатели для оценки рисков нарушения функционирования системы в результате преднамеренного или непреднамеренного воздействия на критичную системную информацию или прикладные программы и пользовательскую информацию, а также рисков, связанных с реализацией техногенных угроз (см. приложение Б);
- показатели для оценки рисков утечки информации о системе или пользовательской информации, распространение которой ограничено в требованиях сторон (заказчика, разработчика, поставщика, пользователей).

Прогнозные показатели для оценки рисков представляют собой вероятности реализации соответствующих угроз за заданное время (период прогноза) в сопоставлении с возможным ущербом. В качестве периода прогноза могут быть выбраны, например, заданный период времени, в течение которого ожидаются несанкционированные информационно-технические воздействия на систему, или продолжительность одной или нескольких стадий жизненного цикла системы. Показатели разделяют на интегральные и частные.

Интегральные показатели рассчитывают при оценке рисков применительно ко всему жизненному циклу системы и всем существенным угрозам без учета мер ЗИ, предлагаемых к использованию в ходе обоснования системных требований, и с учетом применения таких мер. При этом меры ЗИ учитывают в расчетах частных показателей. Номенклатура интегральных показателей риска, рассчитываемых в процессе определения системных требований с учетом необходимости ЗИ в системе, и их взаимосвязь с частными показателями приведена на рисунке Г.1.

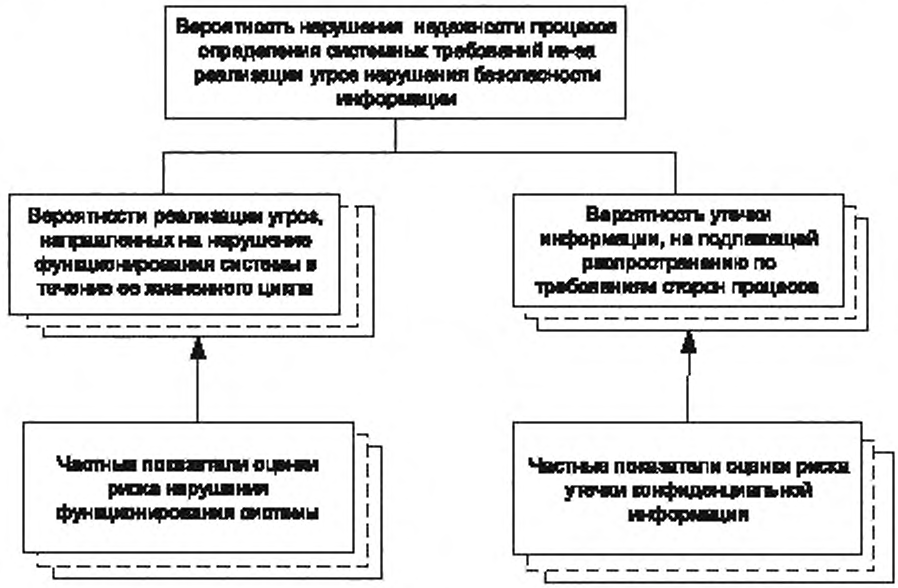


Рисунок Г.1 — Взаимосвязь интегральных и частных показателей

Методы и модели для расчета интегральных показателей приведены в приложении Д.

Частные показатели для оценки рисков рассчитывают применительно к одному или нескольким стадиям жизненного цикла системы, к отдельным угрозам или к выбранной их совокупности, а также применительно к одной или нескольким мерам защиты информации и при отсутствии таких мер.

При проведении оценок рисков соответствующим вероятностным показателям сопоставляют возможный ущерб. Номенклатура и взаимосвязь частных показателей риска, рассчитываемых в процессе определения системных требований с учетом необходимости ЗИ в системе, приведена на рисунке Г.2. Вероятностные показатели мер ЗИ позволяют рассчитать возможное увеличение времени реализации угрозы.

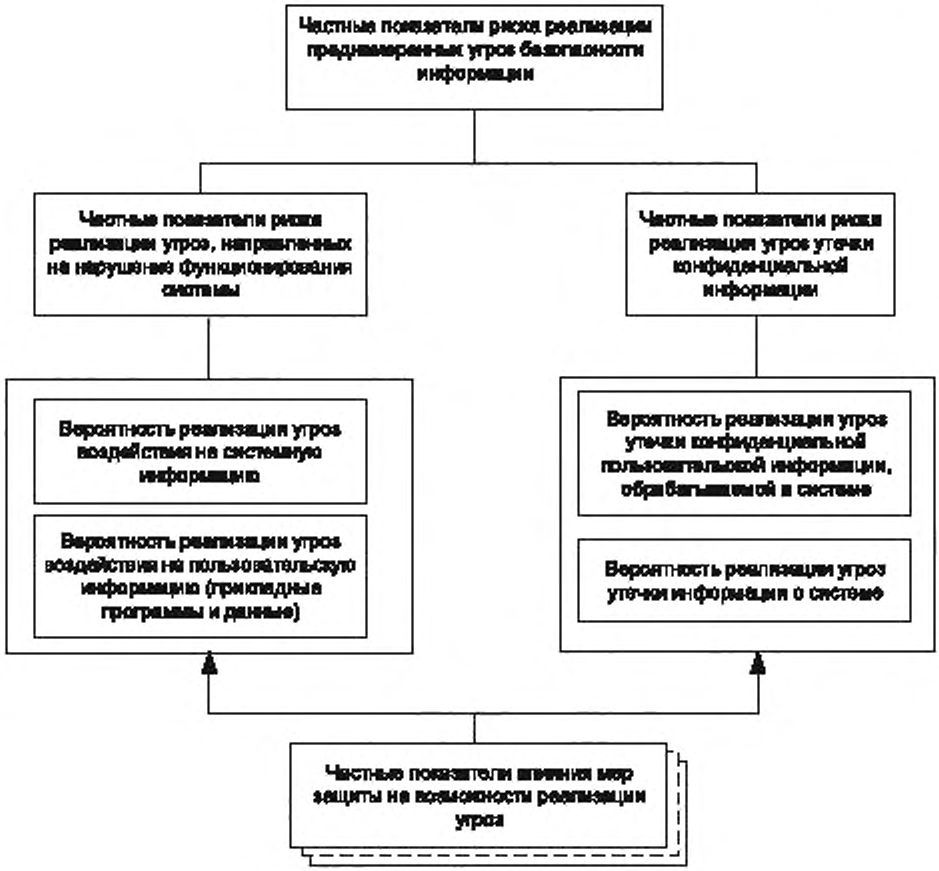


Рисунок Г.2 — Взаимосвязь частных показателей

Модели для расчета таких показателей влияния мер защиты разрабатывают одновременно с моделями для оценки риска реализации угроз (см. приложение Д).

Г.3 Показатели эффективности ЗИ определяют степень отклонения защищенности системы или информации в ней от требуемого уровня защищенности в соответствии с установленной нормой (например, отклонение от установленного предельно допустимого риска реализации угроз в системе).

Г.3.1 Показатели эффективности ЗИ рассчитывают на основе показателей риска реализации угроз для условий без применения и при применении мер защиты, предусматриваемых в процессе определения системных требований. Расчет может проводиться:

- применительно к одной угрозе безопасности информации (угрозе нарушения функционирования системы или угрозе утечки информации) и одной или нескольким мерам защиты, предлагаемым к применению в процессе определения системных требований в интересах парирования (нейтрализации) этой угрозы;

- применительно к определенной совокупности или ко всем выявленным угрозам безопасности информации и совокупности мер защиты, предлагаемых к использованию в процессе определения системных требований в интересах парирования этих угроз.

Для оценки эффективности защиты информации в системе используют разностные, относительные и разностно-относительные показатели — см. 6.3.

Г.3.2 Разностные показатели, представляющие собой разность между достигаемым в условиях применения мер защиты значением вероятности реализации угрозы нарушения надежности реализации процесса определения системных требования ($P_{пр}^{(зи)}$), нарушения функционирования системы ($P_{ф}^{(зи)}$) или утечки конфиденциальной информации ($P_{конф}^{(зи)}$) и требуемыми значениями (не превышающими установленные предельно допустимые значения) этих вероятностей ($P_{пр}^{(тр)}$, $P_{ф}^{(тр)}$ и $P_{конф}^{(тр)}$ соответственно) используют:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(раз)} = \begin{cases} P_{пр}^{(зи)} - P_{пр}^{(тр)}, \text{ если } P_{пр}^{(зи)} > P_{пр}^{(тр)}; \\ 0, \text{ если } P_{пр}^{(зи)} \le P_{пр}^{(тр)}; \end{cases} \quad (Г.1)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{функ}^{(раз)} = \begin{cases} P_{ф}^{(зи)} - P_{ф}^{(тр)}, \text{ если } P_{ф}^{(зи)} > P_{ф}^{(тр)}; \\ 0, \text{ если } P_{ф}^{(зи)} \le P_{ф}^{(тр)}; \end{cases} \quad (Г.2)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(раз)} = \begin{cases} P_{конф}^{(зи)} - P_{конф}^{(тр)}, \text{ если } P_{конф}^{(зи)} > P_{конф}^{(тр)}; \\ 0, \text{ если } P_{конф}^{(зи)} \le P_{конф}^{(тр)}. \end{cases} \quad (Г.3)$$

Максимальная эффективность, оцениваемая по разностному показателю, соответствует его нулевому значению (т. е. вероятность реализации угрозы не превышает предельно допустимого значения). С точки зрения интерпретации разностных показателей это означает, что, если вероятность реализации оцениваемой угрозы ниже требуемой, этой угрозой можно пренебречь. При этом отклонение от требуемого значения вероятности полагают отсутствующим.

Г.3.3 Относительные показатели, представляющие собой отношение предельно допустимых значений вероятности реализации угрозы нарушения надежности реализации процесса определения системных требования $\left(P_{пр}^{(тр)}\right)$, нарушения функционирования системы $(P_{ф}^{(тр)})$ или утечки конфиденциальной информации $\left(P_{конф}^{(тр)}\right)$ к достигаемым в условиях применения мер защиты их значениям (не равным 0), используют соответственно:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(отн)} = \begin{cases} P_{пр}^{(тр)} / P_{пр}^{(зи)}, \text{ если } P_{пр}^{(зи)} > 0 \text{ и } P_{пр}^{(зи)} > P_{пр}^{(тр)}; \\ 1, \text{ если } P_{пр}^{(зи)} > 0 \text{ и } P_{пр}^{(зи)} \le P_{пр}^{(тр)}; \end{cases} \quad (Г.4)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{ф}^{(отн)} = \begin{cases} P_{ф}^{(тр)} / P_{ф}^{(зи)}, \text{ если } P_{ф}^{(зи)} > 0 \text{ и } P_{ф}^{(зи)} > P_{ф}^{(тр)}; \\ 1, \text{ если } P_{ф}^{(зи)} > 0 \text{ и } P_{ф}^{(зи)} \le P_{ф}^{(тр)}; \end{cases} \quad (Г.5)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(отн)} = \begin{cases} P_{конф}^{(тр)} / P_{конф}^{(зи)}, \text{ если } P_{конф}^{(зи)} > 0 \text{ и } P_{конф}^{(зи)} > P_{конф}^{(тр)}; \\ 1, \text{ если } P_{конф}^{(зи)} > 0 \text{ и } P_{конф}^{(зи)} \le P_{конф}^{(тр)}. \end{cases} \quad (Г.6)$$

Максимальная эффективность, оцениваемая по относительному показателю, соответствует его единичному значению (вероятность реализации угрозы не превосходит предельно допустимого ее значения).

Г.3.4 Разностно-относительные показатели, представляющие собой отношение разности между достигаемым значением расчетной вероятности реализации угрозы нарушения надежности реализации процесса определения системных требования $(P_{пр}^{(зи)})$, нарушения функционирования системы $(P_{ф}^{(зи)})$ или утечки конфиденциальной информации $(P_{конф}^{(зи)})$ и предельно допустимым значением этой вероятности к достигаемому значению расчетной вероятности (не равной 0), используют соответственно:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(ро)} = \begin{cases} \left[P_{пр}^{(зи)} - P_{пр}^{(тр)}\right] / P_{пр}^{(зи)}, \text{ если } P_{пр}^{(зи)} > P_{пр}^{(тр)}; \\ 0, \text{ если } P_{пр}^{(зи)} \le P_{пр}^{(тр)}; \end{cases} \quad (Г.7)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{ф}^{(ро)} = \begin{cases} \left[P_{ф}^{(зи)} - P_{ф}^{(тр)}\right] / P_{ф}^{(зи)}, \text{ если } P_{ф}^{(зи)} > P_{ф}^{(тр)}; \\ 0, \text{ если } P_{ф}^{(зи)} \le P_{ф}^{(тр)}; \end{cases} \quad (Г.8)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(ро)} = \begin{cases} \left[P_{конф}^{(зи)} - P_{конф}^{(тр)} \right] / P_{конф}^{(зи)}, \text{ если } P_{конф}^{(зи)} > P_{конф}^{(тр)}, \\ 0, \text{ если } P_{конф}^{(зи)} \le P_{конф}^{(тр)}. \end{cases} \quad (Г.9)$$

Эффективность защиты, оцениваемая по разностно-относительному показателю, тем выше, чем меньше отклонение вероятности реализации угрозы в сторону увеличения от требуемого ее значения.

Г.3.5 Кроме того, при сравнении мер защиты между собой могут применяться показатели эффективности, с использованием которых сравнивают риски, определяемые для условий без применения мер защиты и в условиях применения мер защиты информации, предлагаемых в ходе обоснования системных требований. Такие показатели позволяют оценить, какая из выбираемых мер в наибольшей степени способствует снижению риска, т. е. обладает большей эффективностью.

Соотношения для расчета разностных показателей имеют вид:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(раз)} = P_{пр} - P_{пр}^{(зи)} \text{ при } P_{пр} \ge P_{пр}^{(зи)}; \quad (Г.10)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{ф}^{(раз)} = P_{ф} - P_{ф}^{(зи)} \text{ при } P_{ф} \ge P_{ф}^{(зи)}; \quad (Г.11)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(раз)} = P_{конф} - P_{конф}^{(зи)} \text{ при } P_{конф} \ge P_{конф}^{(зи)}; \quad (Г.12)$$

где $P_{пр}$, $P_{ф}$ и $P_{конф}$ — соответствующие показатели риска при отсутствии оцениваемых мер защиты информации;

$P_{пр}^{(зи)}$, $P_{ф}^{(зи)}$ и $P_{конф}^{(зи)}$ — соответствующие показатели риска в случае применения оцениваемых мер защиты информации.

Соотношения для расчета относительных показателей имеют вид:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(отн)} = P_{пр}^{(зи)} / P_{пр} \text{ при } P_{пр} > 0 \text{ и } P_{пр}^{(зи)} \le P_{пр}; \quad (Г.13)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{ф}^{(отн)} = P_{ф}^{(зи)} / P_{ф} \text{ при } P_{ф} > 0 \text{ и } P_{ф}^{(зи)} \le P_{ф}; \quad (Г.14)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(отн)} = P_{конф}^{(зи)} / P_{конф} \text{ при } P_{конф} > 0 \text{ и } P_{конф}^{(зи)} \le P_{конф}, \quad (Г.15)$$

Примечание — При оценках принято предположение, что вводимые меры защиты не повышают вероятность реализации угрозы.

Аналогичные соотношения имеют место для относительно-разностных показателей:

- для оценки обеспечения надежности реализации процесса определения системных требований

$$\eta_{пр}^{(ор)} = \left(P_{пр} - P_{пр}^{(зи)} \right) / P_{пр}, \text{ при } P_{пр} > P_{пр}^{(зи)}; \quad (Г.16)$$

- для оценки эффективности защиты от нарушений функционирования системы

$$\eta_{ф}^{(ор)} = (P_{ф} - P_{ф}^{(зи)}) / P_{ф} \text{ при } P_{ф} > P_{ф}^{(зи)}; \quad (Г.17)$$

- для оценки эффективности защиты от угроз утечки конфиденциальной информации

$$\eta_{конф}^{(ор)} = \left(P_{конф} - P_{конф}^{(зи)} \right) / P_{конф} \text{ при } P_{конф} > P_{конф}^{(зи)}. \quad (Г.18)$$

Г.3.6 Пример Г.1. Пусть системные требования для проектирования некоторой новой государственной информационной системы определяются в соответствии с положениями настоящего стандарта. Согласно условиям федерального закона [2] система будет относиться к значимым объектам критической информационной инфраструктуры. С учетом требований ГОСТ Р 27002 и нормативных правовых актов [7], [10] и [12] требуется оценить риски реализации угроз безопасности информации на стадии эксплуатации системы, выбрать меры ЗИ и оценить их эффективность. Согласно сформированной модели угроз обусловлено, что путем проникновения в операционную среду системы из сети Интернет на стадии эксплуатации возможна реализация угрозы несанкционированного копирования конфиденциальной информации, к которой отнесены сведения служебного характера и персональные данные сотрудников. Продолжительность стадии эксплуатации ($T_{эксп}$) составляет не менее

пяти лет (т. е. около 43800 часов). Согласно возможному сценарию проникновение в операционную среду системы может быть обеспечено применением пароля, установленного на вход в систему и перехватываемого предварительно внедренной в систему программной закладкой. При проектировании системы предложено применить дополнительно в качестве меры ЗИ аутентификацию пользователей по паролю при обращении к файлам, содержащим конфиденциальную информацию (в дополнение к паролю для доступа в операционную среду системы). Нарушитель, проникнув в операционную среду, для получения доступа к нужному файлу, вынужден подобрать пароль с целью последующего копирования файла и передачи его копии в сеть Интернет по нужному ему адресу.

При формировании модели угроз для системы в соответствии с [7], [10] установлено, что среднее время (τ_∂) между попытками доступа в систему нарушителя, копирования и передачи данных составляет 30 суток, т. е. 720 часов. При отсутствии указанной меры ЗИ риск реализации угрозы оценивается вероятностью $P_{\text{конф}} = 1 - \exp(-T_{\text{экспл}}/\tau_\partial)$, *а в случае ее применения — вероятностью*

$$P_{\text{конф}}^{(\text{зи})} = 1 - \exp\left[-T_{\text{экспл}} / \left(\tau_{\text{пар}} / P_{\text{пар}} + \tau_\partial\right)\right],$$

где $\tau_{\text{пар}}$ — *средняя продолжительность одной попытки подбора пароля длиной восемь символов из букв русского алфавита и цифр, составляющая с применением специальных современных программ подбора пароля путем прямого перебора порядка 4 минут;*

$P_{\text{пар}}$ — *вероятность подбора пароля, составляющая для современных средств подбора примерно* 10^{-8}.

Примечание — При моделировании использовано предположение об экспоненциальной аппроксимации функции распределения времени реализации угрозы. Другие модели см., например, в ГОСТ Р 59341.

Подставляя в правую часть формул для расчета вероятностей $P_{\text{конф}}$ *и* $P_{\text{конф}}^{(\text{зи})}$ *значения параметров* $T_{\text{экспл}}$, τ_∂, $\tau_{\text{пар}}$ *и* $P_{\text{пар}}$, *получаем* $P_{\text{конф}} = 1 - \exp[-43800/720] \approx 1$ *и*

$$P_{\text{конф}}^{(\text{зи})} = 1 - \exp\left[-43800 / \left(\frac{4}{60} \cdot 10^{-8} + 720\right)\right] = 6{,}53 \cdot 10^{-3}.$$

Необходимо оценить эффективность предлагаемой меры ЗИ:

- на основе сравнения вероятности реализации угрозы копирования информации в условиях применения меры ЗИ с требуемым ее значением, установленным в рамках примера на уровне $P_{\text{конф}}^{(\text{тр})} = 10^{-4}$;

- на основе сравнения вероятностей реализации угрозы без меры ЗИ и в условиях применения данной меры.

Результаты расчета эффективности ЗИ путем сравнения достигаемой вероятности реализации угрозы в условиях применения меры ЗИ с ее требуемым значением в соответствии с формулами (Г.3, Г.6 и Г.9) имеют вид:

- по разностному показателю: $\eta_{\text{конф}}^{(\text{раз})} = 6{,}53 \cdot 10^{-3} - 10^{-4} = 6{,}43 \cdot 10^{-3}$;

- по относительному показателю: $\eta_{\text{конф}}^{(\text{отн})} = \dfrac{10^{-4}}{6{,}53 \cdot 10^{-3}} = 1{,}5 \cdot 10^{-2}$;

- по разностно-относительному показателю: $\eta_{\text{конф}}^{(\text{ро})} = \dfrac{6{,}53 \cdot 10^{-3} - 10^{-4}}{6{,}53 \cdot 10^{-3}} = 0{,}985$.

Результаты расчетов эффективности меры ЗИ на основе сравнения вероятности реализации угрозы для условий без применения и с применением мер ЗИ в соответствии с формулами (Г.12, Г.15 и Г.18) имеют вид:

- по разностному показателю: $\eta_{\text{конф}}^{(\text{раз})} = 1 - 6{,}53 \cdot 10^{-3} \approx 0{,}993$;

- по относительному показателю: $\eta_{\text{конф}}^{(\text{отн})} = \dfrac{6{,}53 \cdot 10^{-3}}{1} \approx 0{,}006$;

- по разностно-относительному показателю: $\eta_{\text{конф}}^{(\text{ро})} = \dfrac{1 - 6{,}53 \cdot 10^{-3}}{1} \approx 0{,}993$.

Согласно приведенным результатам расчетов вероятность реализации угрозы в условиях применения мер защиты информации заметно ниже ее требуемого значения, при этом эффективность по разностному и разностно-относительному показателям близка к единице, а по относительному показателю свидетельствует об отсутствии существенных отклонений от требуемого ее предельно допустимого значения.

Приложение Д
(справочное)

Типовые методы и модели для прогнозирования рисков

Д.1 Общие положения

Д.1.1 С учетом необходимости решения вопросов ЗИ в ходе системного анализа должна проводиться оценка рисков нарушения надежности реализации процесса определения системных требований в целом и рисков реализации угроз безопасности информации в системе в течение всего ее жизненного цикла — см. Д.2—Д.5, а также модели, рекомендуемые ГОСТ Р 59349.

Д.1.2 Риск реализации угрозы должен оцениваться с учетом всех факторов, критично влияющих на возможность реализации угроз. Например, к таким факторам относятся:

- существенность рассматриваемых угроз, выражаемая в неприемлемом ущербе от возможной реализации угрозы в данной системе (см. приложение Ж);
- направленность угроз безопасности информации, реализация которых может приводить как к нарушению функционирования системы или отдельных ее программных и/или программно-аппаратных элементов (например, к уничтожению программ, команд и данных, их блокированию, перемещению, модификации), так и к несанкционированному копированию информации, не подлежащей распространению, и/или к несанкционированному запуску приложений;
- фактор времени, когда необходимо учитывать вероятностно-временные характеристики попыток реализации угроз и реакции системы защиты на эти попытки, продолжительность этапов жизненного цикла системы, в течение которых могут быть реализованы угрозы;
- возможность использования в ходе функционирования системы данных о системе, собираемых на предыдущих стадиях жизненного цикла;
- состав и характеристики принимаемых мер защиты информации, общесистемного и прикладного программного обеспечения системы.

Более высокая адекватность оценки рисков, обусловленная необходимостью учета фактора времени, достигается при наличии корректных исходных данных по временным характеристикам нарушения надежности реализации процесса определения системных требований в целом и характеристикам реализации угроз безопасности в системе. Для получения таких данных могут быть использованы результаты анализа прецедентов, а также результаты экспериментальных исследований нарушения надежности функционирования аналогичных систем и реализации угроз безопасности информации в них.

Д.1.3 При оценке риска появление и реализация угроз формально могут быть рассмотрены как совокупности последовательно выполняемых действий, таких как:

- изучение и анализ объекта для реализации угроз безопасности информации в системе;
- формирование условий для «успешной» реализации угроз (например, несанкционированного повышения привилегий, изменения учетных записей, внедрения вредоносной программы), в том числе выявление наличия уязвимостей в системном или прикладном программном обеспечении системы и, прежде всего, в мерах и средствах защиты;
- получение тем или иным способом непосредственного доступа при наличии физического доступа нарушителя к элементам информационной системы (серверу, рабочим станциям, коммуникационным устройствам) или удаленного доступа (по сети) в операционную среду системы;
- получение доступа к командам операционной системы, поиск необходимой информации и выполнение несанкционированных действий (например, копирования, модификации, уничтожения, перемещения);
- передача большого количества пакетов сообщений, передача специально сформированных пакетов, обработка которых приводит к нарушению функционирования системы;
- сокрытие следов реализации угроз (например, записей в журналах, изменений в системном реестре).

Примечание — Словосочетание «успешности» реализации угроз здесь и далее употребляется в кавычках, т. к. при проведении системного анализа «успешная» реализация угроз рассматривается с позиции опасного воздействия на моделируемую систему для определения эффективных мер, средств и способов противодействия этой «успешности».

Д.1.4 Оценка риска реализации угроз безопасности информации должна проводиться как в условиях применения штатных мер ЗИ, так дополнительных мер, определение состава и характеристик которых осуществляют в процессе определения системных требований. Для оценки влияния технических мер должны быть разработаны соответствующие модели, в т. ч. модели для оценки риска реализации угроз, учитывающие способы преодоления или обхода рассматриваемых мер и средств ЗИ — см. Д.3—Д.5.

Д.2 Модель для оценки рисков нарушения надежности реализации процесса определения системных требований в части защиты информации

Д.2.1 Риски нарушения надежности реализации процесса определения системных требований в части ЗИ включают в себя риски нарушения функционирования системы и риски утечки информации о системе или информации, обрабатываемой в системе на каждой стадии и в течение всего ее жизненного цикла. Эти риски оценивают соответствующими вероятностями.

Примечание — При использовании вероятностных моделей делается предположение о повторяемости событий.

Вероятность нарушения надежности реализации процесса определения системных требований $P_{пр}(T_{экспл})$ в части ЗИ применительно к стадии эксплуатации системы (в т. ч. стадии сопровождения) продолжительностью $T_{экспл}$ при наличии на этой стадии U угроз безопасности информации, направленных на нарушение функционирования системы или на хищение конфиденциальной информации, рассчитывают по формуле

$$P_{пр}(T_{экспл}) = 1 - \prod_{u=1}^{U}\left[1 - P_u(T_{эксп\,л} / T_s)\right], \quad (Д.1)$$

где $P_u(T_{эксп\,л}/T_s)$ — условная вероятность того, что на стадии эксплуатации продолжительностью $T_{экспл}$ будет реализована u-я угроза при условии, что хотя бы на одной из предыдущих s-х стадий жизненного цикла или на стадии эксплуатации ($s \le i$, i — условный номер стадии эксплуатации) будет реализована хотя бы одна угроза, в результате чего произойдет утечка информации о системе или внедрена вредоносная программы, позволяющая реализовать u-ю угрозу безопасности информации на стадии эксплуатации. Расчет осуществляют по формуле

$$P_u(T_{эксп\,л} / T_s) = P_u(T_{экспл})\left\{1 - \prod_{s \le I}\prod_{j(u)=1}^{J(u,\,s)}\left[1 - P_{j(u)}(T_s)\right]\right\}, \quad (Д.2)$$

где $P_u(T_{экспл})$ — вероятность того, что угроза на стадии эксплуатации системы продолжительностью $T_{экспл}$ будет реализована при наличии необходимой информации, добытой или на стадии эксплуатации, или на одной из предыдущих стадий, или в результате внедрения на этих стадиях вредоносной программы;

$P_{j(u)}(T_s)$ — вероятность реализации $j(u)$-й угрозы утечки информации на s-й стадии жизненного цикла продолжительностью T_s (предшествующей стадии эксплуатации с номером i или на стадии эксплуатации), необходимой для реализации u-й угрозы на стадии эксплуатации системы, $j(u) = 1, \ldots, J(u, s)$;

$J(u, s)$ — количество угроз на s-й стадии жизненного цикла, реализация которых может привести к утечке информации, используемой для реализации u-й угрозы на стадии эксплуатации системы.

Если угрозы, направленные на нарушение функционирования системы, и угрозы утечки конфиденциальной информации учитывают раздельно, формула (Д.2) имеет следующий вид:

- если информация, используемая для реализации угрозы нарушения функционирования системы, добывается на стадии эксплуатации, то

$$P_{фu}(T_{эксп\,л}/T_s) = P_{фu}(T_{эксп\,л}); \quad (Д.3)$$

- если информация, используемая для реализации угрозы нарушения функционирования системы на стадии эксплуатации, добывается на предыдущих стадиях, то

$$P_{фu}(T_{эксп\,л} / T_s) = P_{фu}(T_{эксп\,л})\left\{1 - \prod_{s<I}\prod_{j(u)=1}^{J(u,\,s\,\text{ф})}\left[1 - P^{(s)}_{ф\,j(u)}(T_s)\right]\right\}; \quad (Д.4)$$

- если информация, используемая для реализации угрозы хищения конфиденциальной информации на стадии эксплуатации, добывается на этой же стадии, то

$$P_{конф\,u}(T_{эксп\,л}/T_s) = P_{конф\,u}(T_{эксп\,л}); \quad (Д.5)$$

- если информация, используемая для реализации угрозы хищения конфиденциальной информации на стадии эксплуатации, добывается на предыдущих стадиях, то

$$P_{конф\ u}(T_{эксп\,л} / T_s) = P_{конф\ u}(T_{эксп\,л})\left\{1 - \prod_{s<I}\prod_{j(u)=1}^{J(u,\,s,\,конф)}\left[1 - P^{(s)}_{конф\ j(u)}(T_s)\right]\right\}, \quad (Д.6)$$

где $P_{фu}(T_{эксп\,л})$ и $P_{конфu}(T_{эксп\,л})$ — соответственно вероятности реализации угроз нарушения функционирования и утечки конфиденциальной информации на стадии эксплуатации системы (в т. ч. стадии сопровождения);

$P^{(s)}_{\text{ф } j(u)}(T_s)$ — вероятность реализации угрозы на s-й стадии, предшествующей или соответствующей стадии эксплуатации (в т. ч. стадии сопровождения), в результате чего произойдет утечка информации о системе или осуществлено потенциально опасное изменение (например, внедрена вредоносная программа), что позволит реализовать u-ю угрозу нарушения функционирования системы на стадии эксплуатации;

$P^{(s)}_{\text{конф } j(u)}(T_s)$ — вероятность реализации угрозы на s-й стадии, предшествующей или соответствующей стадии эксплуатации (в т. ч. стадии сопровождения), в результате чего произойдет утечка информации о системе или осуществлено потенциально опасное изменение (например, внедрена вредоносная программа), что позволит реализовать u-ю угрозу утечки информации о системе или обрабатываемой в системе на стадии эксплуатации;

$J(u, s, \varphi)$ — общее количество угроз утечки информации (или внедрения вредоносной программы) на s-й стадии жизненного цикла системы, предшествующей стадии эксплуатации, необходимой для реализации u-й угрозы нарушения функционирования системы на стадии эксплуатации;

$J(u, s, \text{конф})$ общее количество угроз утечки информации (или внедрения вредоносной программы) на s-й стадии жизненного цикла системы, предшествующей стадии эксплуатации, необходимой для реализации на стадии эксплуатации u-й угрозы утечки информации о системе или информации, обрабатываемой в системе.

Вероятность $P_{\text{ф } u}(T_{\text{экспл}})$ того, что на стадии эксплуатации будет добыта информация о системе, необходимая для последующей реализации на этой же стадии угроз нарушения ее функционирования, и вероятность $P_{\text{конф } u}(T_{\text{экспл}})$ утечки конфиденциальной информации рассчитывают по сходным формулам:

- если $\lambda^{\text{у}}_{\text{ф } u} \neq \lambda^{\text{у}}_{\text{ф доб}}$, то

$$P_{\text{ф } u}(T_{\text{экспл}}) = 1 - \lambda^{\text{у}}_{\text{ф } u} \cdot [\lambda^{\text{у}}_{\text{ф } u} - \lambda^{\text{у}}_{\text{ф доб}}]^{-1} \cdot \exp[-\lambda^{\text{у}}_{\text{ф доб}} \cdot T_{\text{экспл}}] + \lambda^{\text{у}}_{\text{ф доб}} \cdot [\lambda^{\text{у}}_{\text{ф } u} - \lambda^{\text{у}}_{\text{ф доб}}]^{-1} \cdot \exp[-\lambda^{\text{у}}_{\text{ф } u} \cdot T_{\text{экспл}}]; \quad (Д.7)$$

- если $\lambda^{\text{у}}_{\text{ф } u} = \lambda^{\text{у}}_{\text{ф доб}}$, то

$$P_{\text{ф } u}(T_{\text{экспл}}) = 1 - (1 + \lambda^{\text{у}}_{\text{ф } u} \cdot T_{\text{экспл}}) \cdot \exp(-\lambda^{\text{у}}_{\text{ф } u} \cdot T_{\text{экспл}}); \quad (Д.8)$$

- если $\lambda^{\text{у}}_{\text{конф } u} \neq \lambda^{\text{у}}_{\text{конф доб}}$, то

$$P_{\text{конф } u}(T_{\text{экспл}}) = 1 - \lambda^{\text{у}}_{\text{конф } u} \cdot [\lambda^{\text{у}}_{\text{конф } u} - \lambda^{\text{у}}_{\text{конф доб}}]^{-1} \cdot \exp[-\lambda^{\text{у}}_{\text{конф доб}} \cdot T_{\text{экспл}}] + \lambda^{\text{у}}_{\text{конф доб}} \cdot [\lambda^{\text{у}}_{\text{конф } u} - \lambda^{\text{у}}_{\text{конф доб}}]^{-1} \cdot \exp[-\lambda^{\text{у}}_{\text{конф } u} \cdot T_{\text{экспл}}]; \quad (Д.9)$$

- если $\lambda^{\text{у}}_{\text{конф } u} = \lambda^{\text{у}}_{\text{конф доб}}$, то

$$P_{\text{конф } u}(T_{\text{экспл}}) = 1 - (1 + \lambda^{\text{у}}_{\text{конф } u} \cdot T_{\text{экспл}}) \cdot \exp(-\lambda^{\text{у}}_{\text{конф } u} \cdot T_{\text{экспл}}); \quad (Д.10)$$

где $\lambda^{\text{у}}_{\text{ф } u}$ и $\lambda^{\text{у}}_{\text{конф } u}$ — соответственно ожидаемые интенсивности «успешных» попыток реализации угроз на стадии эксплуатации системы, связанных с нарушением функционирования системы и утечкой информации, подлежат определению с использованием соотношений

$$\lambda^{\text{у}}_{\text{ф } u} = \lambda_{\text{ф } u} \cdot R_{\text{ф } u} \text{ и } \lambda^{\text{у}}_{\text{конф } u} = \lambda_{\text{конф } u} \cdot R_{\text{конф } u}; \quad (Д.11)$$

где $\lambda_{\text{ф } u}$ и $\lambda_{\text{конф } u}$ — соответственно ожидаемые интенсивности попыток реализации угроз на стадии эксплуатации системы, связанных с нарушением ее функционирования и утечкой конфиденциальной информации (подлежат определению для осуществления моделирования);

$R_{\text{ф } u}$ и $R_{\text{конф } u}$ — вероятности того, что в каждой попытке угроза, направленная соответственно на нарушение функционирования системы и утечку конфиденциальной информации, будет реализована на стадии эксплуатации системы (этими вероятностями оценивается и влияние мер защиты на возможности реализации указанных угроз);

$\lambda^{\text{у}}_{\text{ф доб}}$ и $\lambda^{\text{у}}_{\text{конф доб}}$ — соответственно ожидаемые интенсивности «успешных» попыток реализации угроз на стадии эксплуатации системы, связанных с добыванием информации о системе в интересах нарушения ее функционирования и утечкой конфиденциальной информации, подлежат определению с использованием соотношений

$$\lambda^{\text{у}}_{\text{ф доб}} = \lambda_{\text{ф доб}} \cdot R_{\text{ф доб}} \text{ и } \lambda^{\text{у}}_{\text{конф доб}} = \lambda_{\text{конф доб}} \cdot R_{\text{конф доб}}; \quad (Д.12)$$

$\lambda_{\text{ф доб}}$ и $\lambda_{\text{конф доб}}$ — соответственно ожидаемые интенсивности попыток реализации угроз на стадии эксплуатации системы, связанных с добыванием информации, используемой для нарушения функционирования системы и выявлением конфиденциальной информации (подлежат определению для осуществления моделирования);

$R_{ф\ доб}$ и $R_{конф\ доб}$ — вероятности того, что в каждой попытке угроза выявления информации о системе, необходимой для последующего нарушения ее функционирования или, соответственно, хищения конфиденциальной информации, будет реализована на стадии эксплуатации системы (этими вероятностями оценивается и влияние мер защиты на возможности реализации указанных угроз).

Вероятности $P_{ф\ u}(T_{эксплл})$, $P_{конф\ u}(T_{эксплл})$, $P^{(s)}_{ф\ j(u)}(T_s)$ и $P^{(s)}_{конф\ j(u)}(T_s)$ в случае, когда информация о системе, необходимая для реализации угроз, имеется, определяют по следующим формулам:

$$P_{ф\ u}(T_{эксплл}) = 1 - \exp[-\lambda_{ф\ u} \cdot R_{ф\ u} \cdot T_{эксплл}]; \quad (Д.13)$$

$$P_{конф\ u}(T_{эксплл}) = 1 - \exp[-\lambda_{конф\ u} \cdot R_{конф\ u} \cdot T_{эксплл}]; \quad (Д.14)$$

$$P^{(s)}_{ф\ j(u)}(T_s) = 1 - \exp\left[-\lambda_{ф\ j(u)}(s) \cdot R^{(s)}_{ф\ j(u)} \cdot T_s\right]; \quad (Д.15)$$

$$P^{(s)}_{конф\ j(u)}(T_s) = 1 - \exp\left[-\lambda_{конф\ j}(s) \cdot R^{(s)}_{конф\ j(u)} \cdot T_s\right], \quad (Д.16)$$

где $\lambda_{ф\ j(u)}(s)$ и $\lambda_{конф\ j}(s)$ — соответственно интенсивности попыток реализации угроз на s-й стадии, направленных на утечку информации о системе (или информации, обрабатываемой в системе) или на внедрение вредоносной программы, что позволит реализовать u-ю угрозу нарушения функционирования системы или хищения конфиденциальной информации на стадии эксплуатации (подлежат определению для осуществления моделирования);

$R^{(s)}_{ф\ j(u)}$ и $R^{(s)}_{конф\ j(u)}$ — вероятности того, что в каждой попытке угроза, направленная соответственно на нарушение функционирования системы или на хищение конфиденциальной информации на s-й стадии, будет реализована.

Примечания

1 За счет умножения на вероятности соответственно $R_{ф\ u}$, $R_{конф\ u}$, $R^{(s)}_{ф\ j(u)}$, $R^{(s)}_{конф\ j(u)}$ в формулах (Д.11), (Д.13—Д.16) и на вероятности $R_{ф\ доб}$ и $R_{конф\ доб}$ в формуле (Д.12) происходит «просеивание» потока изначальных попыток реализации угроз. В результате произведения осуществляется прореживание исходного потока попыток, в итоге осуществляется учет лишь «успешных» попыток реализации угроз. В итоге интенсивности «успешных» попыток реализации угроз уменьшаются с изначальных уровней $\lambda_{ф\ u}$, $\lambda_{конф\ u}$, $\lambda_{ф\ j(u)}(s)$ и $\lambda^{(s)}_{конф\ j(u)}$ до уровней $\lambda^{у}_{ф\ u}$, $\lambda^{у}_{конф\ u}$, $\lambda^{у}_{ф\ j(u)}(s)$ и $\lambda^{у}_{конф\ j(u)}(s)$ соответственно. Именно этот эффект «просеивания» отражен в формулах (Д.11)—(Д.16).

2 Значения величин $\lambda_{ф\ u}$, $\lambda_{конф\ u}$, $R_{ф\ u}$, $R_{конф\ u}$, $\lambda_{ф\ j(u)}(s)$, $\lambda_{конф\ j(u)}(s)$, $R^{(s)}_{ф\ j(u)}$, $R^{(s)}_{конф\ j(u)}$ следует указывать в частной модели угроз безопасности информации, разрабатываемой в соответствии с [10], [11] для каждой создаваемой, модернизируемой и подлежащей эксплуатации системы с учетом всех стадий ее жизненного цикла.

3 Для получения статистических данных по $\lambda_{ф\ u}$, $\lambda_{конф\ u}$, $R_{ф\ u}$, $R_{конф\ u}$, $\lambda_{ф\ j(u)}(s)$, $\lambda_{конф\ j(u)}(s)$, $R^{(s)}_{ф\ j(u)}$ и $R^{(s)}_{конф\ j(u)}$, близким к реальности, в качестве вспомогательных средств могут быть использованы технологические стенды или стендовые полигоны, применяемые для оценки достижимых показателей защищенности и устойчивости функционирования систем в имитируемых условиях несанкционированных информационно-технических воздействий — см. ГОСТ Р 59342 и ГОСТ Р 59355.

Д.2.2 Интегральную вероятность нарушения надежности реализации процесса с учетом угроз безопасности информации в течение всего жизненного цикла системы $P_{инт}(T_{жц})$ определяют из соотношения

$$P_{инт}(T_{жц}) = 1 - [1 - P_{пр}(T_{эксплл})] \cdot [1 - P_{конф}(T_{вых})], \quad (Д.17)$$

где $P_{пр}(T_{эксплл})$ — вероятность нарушения надежности реализации процесса определения системных требований в части ЗИ применительно к стадии эксплуатации системы (в т. ч. стадии сопровождения) продолжительностью $T_{эксплл}$ — см. формулу (Д.1);

$P_{конф}(T_{вых})$ — вероятность реализации угрозы утечки информации о системе или информации, полученной в результате ее функционирования, на стадии выведения системы из эксплуатации ($s = 6$) продолжительностью $T_{вых}$

$$P_{конф}(T_{вых}) = 1 - \exp[-\lambda_{вых} \cdot R_{вых} \cdot T_{вых}], \quad (Д.18)$$

где $\lambda_{вых}$ — ожидаемая интенсивность попыток реализации угроз утечки информации на стадии выведения системы из эксплуатации (подлежит определению для осуществления моделирования);

$R_{вых}$ — вероятность утечки информации в каждой попытке реализации угрозы на стадии выведения системы из эксплуатации.

Д.2.3 Пример Д.1. Пусть прогнозируемая продолжительность стадии эксплуатации (s = 4) системы, разрабатываемой для городской администрации, составляет 10 лет ($T_s \equiv T_{экспл}$ = 10 лет = 87600 ч). В системе предполагается обработка конфиденциальной информации, содержащие сведения служебного характера. Система относится к государственной и к ней предъявляются требования по защите информации в соответствии с [3], [10]. В соответствии с разработанной моделью угроз безопасности информации на этапе эксплуатации системы возможна реализация угроз несанкционированного копирования обрабатываемой в ней конфиденциальной информации. Угрозы могут быть реализованы путем проникновения в операционную среду системы и повышения привилегий нарушителем, а также с использованием вредоносной программы, внедряемой на стадии поставки (s = 3) системы заказчику продолжительностью 3 месяца ($T_s \equiv T_{пост}$ = 2160 ч). Если вредоносная программа окажется внедренной, то копирование информации при отсутствии необходимых мер защиты вполне обоснованно можно предположить неизбежным, т. е. без расчетов по формуле (Д.14) $P^{(4)}_{конф2}(T_{эксплл}) \approx$ *1. Положим, по набранной статистике интенсивности попыток реализации угроз в соответствии с моделью угроз для данной системы составляют (для расчетов использована единая шкала для единиц измерения — «раз в час»):*

- для угрозы, реализуемой на стадии эксплуатации путем проникновения в операционную среду, $\lambda_{конф1}(1) = 1{,}4 \cdot 10^{-3}$ *(т. е. один раз в месяц);*

- для угрозы внедрения вредоносной программы на стадии поставки $\lambda_{конф1}(3) = 4{,}2 \cdot 10^{-3}$ *(т. е. один раз в десять дней).*

Пусть вероятности реализации каждой угрозы в каждой попытке в соответствии с моделью угроз для данной системы составляют на стадии эксплуатации $R^{(4)}_{конф1} = 10^{-2}$ *и на стадии поставки* $R^{(3)}_{конф1} = 5 \cdot 10^{-3}$*, при этом отсутствует угроза утечки информации на стадии выведения системы из эксплуатации.*

Необходимо рассчитать вероятность нарушения надежности реализации процесса определения системных требований в части ЗИ с учетом угроз безопасности информации $P_{инт}(T_{ж.ц.})$.

Возможно следующее решение для примера Д.1.

Так как угрозы, направленные на нарушение функционирования системы, отсутствуют, то рассчитывается только вероятность утечки информации в соответствии с формулой (Д.16) для s = 4:

$$P^{(4)}_{конф1}(T_{эксплл}) = 1 - \exp\left[-\lambda_{конф1}(4) \cdot R^{(4)}_{конф1} \cdot T_{эксплл}\right] = 1 - \exp\left(-1{,}4 \cdot 10^{-3} \cdot 10^{-2} \cdot 87600\right) = 1 - \exp(-1{,}23) \approx 0{,}71$$

и вероятность внедрения вредоносной программы в соответствии с формулой (Д.16):

$$P^{(3)}_{конф1}(T_{пост}) = 1 - \exp\left[-\lambda_{конф1}(3) \cdot R^{(3)}_{конф1} \cdot T_{пост}\right] = 1 - \exp\left(-4{,}2 \cdot 10^{-3} \cdot 5 \cdot 10^{-3} \cdot 20160\right) \approx 0{,}42.$$

В связи с тем, что угрозы утечки информации о системе на стадии выведения ее из эксплуатации отсутствуют, т. е. $P_{конф}(T_{вых}) = 0$*, то в соответствии с формулой (Д.17):*

$$P_{пр}(T_{эксплл}) = 1 - \left[1 - P^{(4)}_{конф1}(T_{эксплл})\right] \cdot \left[1 - P^{(3)}_{конф1}(T_{пост})\right] = 1 - [1 - 0{,}71] \cdot [1 - 0{,}42] \approx 0{,}83.$$

Таким образом, вероятность нарушения надежности реализации процесса определения системных требований в примере почти в 5 раз превысит вероятность надежного выполнения процесса [0,83/(1 – 0/83) ≈ 4,88]. *В интерпретации системной инженерии такая ожидаемая надежность выполнения рассматриваемого процесса неприемлема, необходим поиск более эффективных мер ЗИ.*

Д.3 Аналитические методы и модели для оценки вероятностей реализации угроз безопасности информации при прогнозировании рисков

Д.3.1 Аналитические методы и модели должны позволять проведение расчетов вероятности реализации всей совокупности существенных угроз безопасности информации на любом из этапов и в течение всего жизненного цикла системы. Для прогнозирования рисков могут применяться любые возможные методы и модели, обеспечивающие приемлемое достижение поставленных целей. Так, при расчетах вероятностей реализации угроз на практике применяют методы теории надежности, теории массового обслуживания, аппарата марковских и полумарковских процессов, аппарата сетей Петри-Маркова с логическими условиями (см. Д.2, Д.3.2, Д.3.3, Д.3.4). Выбор того или иного метода для моделирования определяется формализованным содержанием реализации угрозы для условий без применения и при применении обосновываемых мер защиты.

Д.3.2 Методы теории массового обслуживания применяют в том случае, когда элемент системы, на который осуществляется воздействие в результате реализации угрозы, может быть представлен в виде системы массового обслуживания (СМО), в которую поступает поток «заявок» — например, поток пакетов сообщений, реализующих рассматриваемую угрозу.

Примечание — В зависимости от содержания угрозы, состава и характеристик мер защиты могут применяться для моделирования однолинейные и многолинейные СМО, СМО с отказами и с очередями, с ограничениями и без ограничений на время пребывания заявок в системе, с различными дисциплинами обслуживания и видами приоритетов заявок (например, с относительными, абсолютными приоритетами или с их комбинацией).

В простых моделях суммарный поток заявок на обслуживание часто полагают пуассоновским (из-за большого количества слагающих его составных потоков, вносящих соизмеримый вклад в общий поток). Такой поток характеризуется интенсивностью поступления заявок в систему $\lambda = 1/\tau_{между}$, где $\tau_{между}$ — средняя продолжительность времени между моментами поступления заявок. Для получения пессимистических оценок временных задержек в очередях длительность обслуживания заявок полагают экспоненциально распределенной с интенсивностью обслуживания $\mu = 1/\tau_{обсл}$, где $\tau_{обсл}$ — средняя продолжительность обслуживания одной заявки. В этом случае загрузку однолинейной СМО без ограничений в обслуживании ρ определяют как отношение: $\rho = \lambda/\mu$. В качестве примера применения упрощенной модели ниже описана модель для расчета вероятности реализации угрозы компьютерной атаки, получившей название «шторм TCP-запросов» (Transmission Control Protocol — протокол управления передачей, атаку с его использованием называют также с использованием англоязычного наименования «SYN-flooding»).

Д.3.3 Пример Д.2. Пусть на некотором государственном предприятии проводится модернизация системы, обеспечивающей автоматизацию управления предприятием, в т. ч. в интересах повышения защищенности обрабатываемой в ней информации. В соответствии с требованиями нормативных правовых актов [10], [11] были выявлены возможные угрозы, которые могут быть реализованы. Установлено, что большая часть угроз может быть реализована из сети общего пользования, к которой ранее было подключено большинство компьютеров модернизируемой системы. Положим, для парирования этих угроз было предложено для взаимодействия с заинтересованными инстанциями через сеть общего пользования выделить только один компьютер, отключив от этой сети остальные компьютеры. Однако подключенный компьютер подвержен компьютерным атакам типа «Отказ в обслуживании», одной из которых является атака «Syn-flooding». Суть атаки заключается в том, что на атакуемый компьютер в составе защищаемой системы передается из сети общего пользования большое количество запросов на установление «полуоткрытого» виртуального соединения по выбранному порту. В результате операционная система, ожидая подтверждения (квитанции) о готовности абонента к связи, держит в буфере информацию о предполагаемом соединении, повторяя посылку сообщений — квитанций о получении запроса на соединение. Если запросов на соединение поступило много, а квитанции от атакующего компьютера не последовало, то буфер оказывается полностью заполненным и система перестает принимать другие запросы по данному порту. Необходимо оценить риск реализации данной атаки.

Требуется оценить защищенность такой системы от компьютерных атак.

Возможно следующее решение для примера Д.2.

Компьютерная атака может быть промоделирована с использованием модели системы массового обслуживания с очередью фиксированной длины при следующих условиях: обслуживающий прибор (компьютер) при поступлении рассматриваемых заявок отказывает и может быть восстановлен по мере истечения фиксированного промежутка времени после переполнения буфера (в котором формируется очередь заявок, т. е. поступающих запросов). Вероятность того, что операционная система компьютера к моменту времени t перестанет принимать новые пакеты информации (т.е. заявки, поступающие на прибор), в результате чего компьютерная атака будет реализована, определяют из соотношения:

$$P_u(t) = 1 - \exp(-\lambda_{пак} \cdot t/J_{пред}), \qquad (Д.19)$$

где $\lambda_{пак}$ *— интенсивность поступления пакетов с запросами на соединение (пакетов с установленным флагом SYN в служебном заголовке);*

$J_{пред}$ *— предельное количество возможных соединений по одному порту, при котором буфер оказывается заполненным.*

Среднее время, необходимое для реализации атаки, составляет величину:

$$\tau_u = J_{пред}/\lambda_{пак}. \qquad (Д.20)$$

Положим, что по прецедентному принципу принят следующий критерий блокировки атаки: если атака обнаружена до момента прихода $J_{пред} + 1$ пакета с некоторой вероятностью $P_{обн}$, то атака блокируется. Вероятность реализации атаки рассчитывают по формуле

$$P_u(t) = 1 - \exp[-t \cdot (1 - P_{обн}) \cdot \lambda_{пак}/J_{пред}]. \qquad (Д.21)$$

В графическом виде на рисунке Д.1 представлены аналитические зависимости риска реализации угрозы от возможностей системы (по обнаружению вторжений при атаке «SYN-flooding»), характеризуемых вероятностью обнаружения $P_{обн}$.

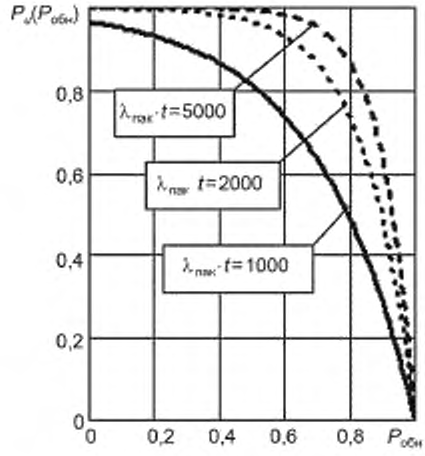


Рисунок Д.1 — Зависимость вероятности реализации компьютерной атаки «SYN-flooding» от вероятности ее обнаружения и блокирования при $J_{пред}$ = 300

Системный анализ результатов расчетов показал:

- при вероятности обнаружения атаки выше условного значения 0,9 и, соответственно, принятия мер по ее пресечению, возможности достижения системой состояния «Отказ в обслуживании» быстро уменьшаются;

- с увеличением интенсивности запросов на соединение существенно растет возможность переполнения буфера операционной системы и реализации рассматриваемой атаки — например, с увеличением интенсивности в 5 раз вероятность реализации атаки возрастает более, чем на 35 %, и достигает 0,95 при $P_{обн}$ = 0,7. В интерпретации системной инженерии вероятность 0,95 означает неизбежность реализации атаки.

Д.3.4 Для моделирования угроз безопасности информации с использованием аппарата марковских и полумарковских процессов применяют в основном процессы с непрерывным временем и дискретными состояниями. При этом отсутствуют логические условия выполнения моделируемого процесса, а также должны быть корректно определены его вероятностно-временные характеристики.

Если имеет место большое количество состояний, то на практике приходится использовать приближенные решения. Для моделей угроз на основе марковских процессов характерно не только отсутствие логических условий реализации угроз безопасности информации, но и действий, выполняемых параллельно.

В общем случае при проведении системного анализа возникновение и реализация угрозы формально представляет собой сумму последовательно выполняемых действий:

$$A_u(t_u) = B_u(\tau_{сбор})\&X_u(\tau_{усл})\&G_u(\tau_{\partial})\&S_u(\tau_{скр}) \text{ и } t_u = \tau_{сбор} + \tau_{усл} + \tau_{\partial} + \tau_{скр}, \quad (Д.22)$$

где $B_u(\tau_{сбор})$ — формализованное описание совокупности действий, связанных со сбором информации за время $\tau_{сбор}$ относительно системы, необходимой для реализации u-й угрозы;

$X_u(\tau_{усл})$ — формализованное описание совокупности действий, направленных на непосредственное формирование необходимых условий для «успешной» реализации u-й угрозы (например, внедрения вредоносной программы, повышения привилегий, изменения настроек системы защиты или блокирования выполнения ею команд и т. д.) в течение времени $\tau_{усл}$;

$G_u(\tau_{\partial})$ — формализованное описание совокупности действий, связанных с реализацией угрозы за время τ_{∂} (например, с проникновением в операционную среду атакуемого компьютера, поиском необходимой информации и выполнением непосредственных несанкционированных действий с пользовательской или системной информацией — уничтожением, блокированием, копированием, модификацией, несанкционированным запуском приложений);

$S_u(\tau_{скр})$ — формализованное описание совокупности действий по скрытию следов реализации угрозы в течение времени $\tau_{скр}$.

В зависимости от целей системного анализа действия по скрытию следов в течение времени $\tau_{скр}$ могут быть включены в этап атакующих действий (если они учитываются при моделировании динамики реализации угроз безопасности информации). Действия, направленные на сбор необходимой информации о системе и непосредственное формирование необходимых условий для «успешной» реализации угрозы, рассматривают как совокупность действий, выполняемых в течение единого времени подготовки к реализации угрозы $\tau_{подг} = \tau_{сбор} + \tau_{усл}$.

Графически марковский процесс представляют в виде ориентированного графа, содержащего состояния процесса и дуги, указывающих направления изменения возможных состояний. Если моделируемый марковский процесс описывается K состояниями, в которые он переходит последовательно в течение рассматриваемого времени, то динамику переходов из состояния в состояние описывают системой стохастических дифференциальных уравнений:

$$\frac{d}{dt}p_j(t) = \sum_{k=1}^{K} \lambda_{kj}(t) \cdot p_k(t),\ j = 1...K, \qquad (Д.23)$$

где $p_j(t)$ — вероятность того, что марковский процесс в момент времени t находится в j-м состоянии;

$\lambda_{kj}(t)$ — интенсивность перехода процесса из состояния k в состояние j, в общем случае зависящая от времени. На практике делают предположение о стационарности марковских процессов, когда указанная интенсивность не зависит от времени и равна λ_{kj}.

Решение системы дифференциальных уравнений (Д.23) позволяет рассчитать вероятность перехода марковского процесса в конечное состояние, соответствующее состоянию реализации угрозы. Именно эта расчетная вероятность характеризует собой вероятность реализации угрозы.

Д.3.5 Пример Д.3. Пусть в ходе проведения мероприятий по модернизации системы защиты информации в автоматизированной системе некоторого органа власти в соответствии с [2], [10]—[12] и ГОСТ Р 27002 проводится анализ и оценка рисков реализации возможных угроз безопасности информации. Одной из таких угроз является угроза несанкционированного доступа, основанного на внедрении программной закладки — вредоносной программы, например, типа «троянский конь». С использованием этой вредоносной программы осуществляется поиск открытых портов, затем перехват пароля, установление соединения с абонентом по сетевому адресу и передача перехваченного пароля для расшифровки. Затем нарушитель захватывает сеанс TCP-соединения и получает доступ в операционную среду компьютера. Тем самым нарушитель достигает цели своей компьютерной атаки.

Требуется оценить возможность реализации угрозы несанкционированного доступа с использованием вредоносной программы типа «троянский конь».

Возможно следующее решение для примера Д.3.

Для оценки вероятности реализации такой атаки используется марковская модель, граф состояний которой приведен на рисунке Д.2.

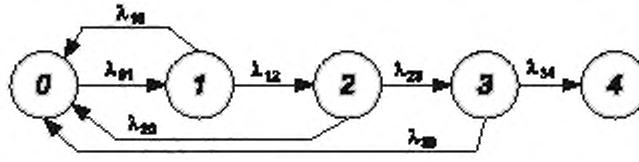


Рисунок Д.2 — Граф, описывающий динамику развития компьютерной атаки, основанной на внедрении программной закладки

На графе используются следующие обозначения:

0 — состояние, когда нарушитель готов к попыткам внедрения программной закладки;

1 — состояние, когда программная закладка внедрена и осуществляется анализ сети (выявление открытых портов);

2 — состояние, когда выявлен открытый порт и программная закладка осуществляет перехват пароля доступа;

3 — состояние, когда пароль доступа перехвачен и программная закладка запрашивает сеанс связи от имени хоста-цели атаки с передачей выявленной информации нарушителю;

4 — состояние, когда сеанс связи с нарушителем установлен, т. е. нарушитель получил доступ в операционную среду компьютера по сети с использованием выявленного порта.

Переход из состояния в состояние описывается системой дифференциальных уравнений:

$$\begin{cases} P_0'(t) = -\lambda_{01}P_0(t) + \lambda_{10}P_1(t) + \lambda_{20}P_2(t) + \lambda_{30}P_3(t); \\ P_1'(t) = \lambda_{01}P_0(t) - \lambda_{12}P_1(t) - \lambda_{10}P_1(t); \\ P_2'(t) = \lambda_{12}P_1(t) - \lambda_{20}P_2(t) - \lambda_{23}P_2(t); \\ P_3'(t) = \lambda_{23}P_2(t) - \lambda_{30}P_3(t) - \lambda_{34}P_3(t); \\ P_4'(t) = \lambda_{34}P_3(t), \end{cases} \qquad (Д.24)$$

где $P'_0(t)$ ... $P'_4(t)$ — производные от вероятностей $P_0(t)$ ... $P_4(t)$ соответственно.

Интенсивности переходов из состояния в состояние и вероятности, характеризующие течение марковского процесса, определяются следующим образом:

$\lambda_{01} = P_{инф}/\tau_{инф}$ — интенсивность внедрения программной закладки;

$P_{инф}$, $\tau_{инф}$ — вероятность и среднее время внедрения программной закладки;

$\lambda_{12} = P_{порт}/\tau_{порт}$ — интенсивность выявления открытого порта;

$P_{порт}$, $\tau_{порт}$ — вероятность и среднее время выявления открытого порта;

$\lambda_{23} = P_{пар}/\tau_{пар}$ — интенсивность выявления пароля;

$P_{пар}$, $\tau_{пар}$ — вероятность и среднее время выявления пароля;

$\lambda_{34} = P_{св}/\tau_{св}$ — интенсивность установления сеанса связи между программной закладкой и нарушителем;

$P_{св}$, $\tau_{св}$ — вероятность и среднее время установления сеанса связи;

$\lambda_{10} = (1 - P_{порт})/\tau_{порт}$ — интенсивность перехода процесса в начальное состояние в случае срыва выявления свободного порта;

$\lambda_{20} = (1 - P_{пар})/\tau_{пар}$ — интенсивность перехода процесса в начальное состояние в случае срыва выявления пароля;

$\lambda_{30} = (1 - P_{св})/\tau_{св}$ — интенсивность перехода процесса в начальное состояние в случае срыва установления сеанса связи между программной закладкой и нарушителем.

При этом вероятность и среднее время подбора пароля за n попыток при прямом переборе определяют по формулам:

$$P_{пар} \approx n/A^w \text{ и } \tau_{пар} = A^w \cdot T_{пар}/2, \qquad (Д.25)$$

где A — число символов в алфавите, на основе которого сформирован пароль;

w — длина пароля;

$T_{пар}$ — время выполнения одной попытки ввода пароля.

Для приведенного графа состояний процесса среднее время перехода в последнее состояние (т. е. среднее время несанкционированного доступа) определяется из полученного путем решения системы дифференциальных уравнений (Д.24) соотношения

$$\tau_{НСД} = (P_{инф} \cdot \tau_{порт} + \tau_{инф})/P_{инф} \cdot P_{порт} \cdot P_{пар} \cdot P_{св} + (P_{пар} \cdot \tau_{св} + \tau_{пар})/P_{пар} \cdot P_{св}, \qquad (Д.26)$$

где $P_{инф} > 0$, $P_{порт} > 0$, $P_{пар} > 0$, $P_{св} > 0$,

При этом если хотя бы одна из этих вероятностей стремится к 0, несанкционированный доступ становится невозможным ($\tau_{НСД} \to \infty$), а вероятность реализации угрозы (например, копирования защищаемой информации) за время t рассчитывают по формуле

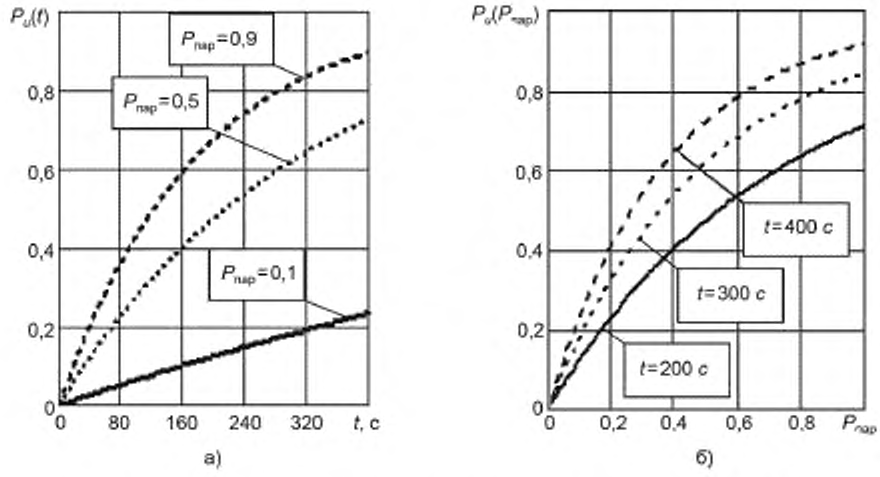
$$P_u(t) = \begin{cases} 1 - \left[\tau_{НСД}/(\tau_{НСД} - \tau_д)\right] \cdot \exp(-t/\tau_{НСД}) + \left[\tau_д/(\tau_{НСД} - \tau_д)\right] \cdot \exp(-t/\tau_д) \text{ при } \tau_{НСД} \neq \tau_д; \\ 1 - \left(1 + \dfrac{t}{\tau_д}\right) \cdot \exp\left(-\dfrac{t}{\tau_д}\right) \text{ при } \tau_{НСД} = \tau_д, \end{cases} \qquad (Д.27)$$

где $\tau_д$ — среднее время выполнения деструктивного действия.

Примечание — При значениях $\tau_{НСД}$, близких к нулю, и значениях $\tau_д$, отличных от 0, вероятность реализации угрозы будет определяться только средним временем выполнения деструктивного действия, т. е. $P_u(t) = 1 - \exp(-t/\tau_д)$. Если среднее время выполнения деструктивного действия тоже стремится к 0, то реализация угрозы неизбежна: вероятность $P_u(t)$ стремится к 1.

Графики зависимости $P_u(t)$ и $P_u(P_{пар})$ при условии неравенства средних времен несанкционированного доступа и выполнения деструктивного действия представлены на рисунке Д.3.

Системный анализ результатов расчетов показал, что с увеличением времени, в течение которого может быть реализована угроза несанкционированного доступа к защищаемой информации, независимо от значения вероятности подбора пароля вероятность реализации угрозы стремится к единице. При ограниченном времени, в течение которого может быть реализована угроза, на возможность ее реализации определяющим образом влияют как вероятность и продолжительность подбора пароля, так и вероятности и времена выявления открытого порта, внедрения программной закладки и установления сеанса связи между программной закладкой и нарушителем.



$\tau_{порт}$ = 2 с, $\tau_{инф}$ = 10 с, $\tau_{св}$ = 10 с, $\tau_{пар}$ = 120 с, $P_{порт}$ = 0,9, $P_{инф}$ = 0,8, $P_{св}$ = 0,9

Рисунок Д.3 — Зависимости вероятности реализации угрозы от времени (а) и вероятности вскрытия пароля (б)

Д.3.6 Для полумарковских процессов (ПМП) характерно наличие:

- разветвлений, при этом выбор ветви, по которой развивается процесс, происходит с заданной вероятностью;
- параллельно выполняемых во времени действий, при этом, как и для марковских процессов, для них отсутствуют логические условия реализации угроз безопасности информации.

Суть ПМП состоит в следующем. Пусть в начальный момент времени $t = 0$ моделируемый процесс находится в состоянии i, $i \in I$ в течение некоторого случайного времени θ_0, после чего процесс мгновенно переходит в состояние j, $j \in I$. Время θ_0 — это случайная величина с произвольной функцией распределения $F_{ij}(t)$, а переход процесса из состояния i в состояние j происходит с вероятностью $\pi_{ij} \geq 0$ с выполнением условия $\sum_{j \in I} \pi_{ij} = 1$.

Если из состояния j процесс переходит в состояние k, $k \in I$, то в состоянии j процесс пребывает случайное время θ_1, имеющее произвольное распределение $F_{jk}(t)$ — см. рисунок Д.4.

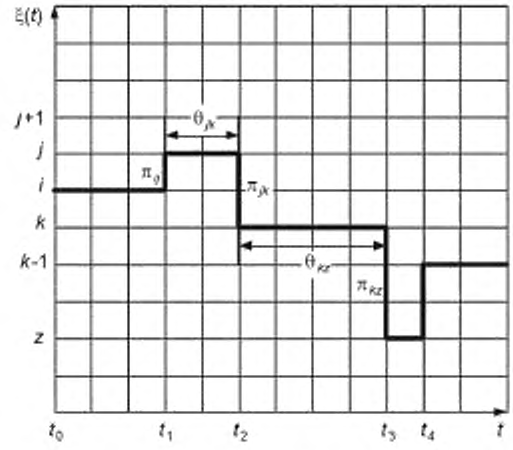


Рисунок Д.4 — Динамика протекания полумарковского процесса

ПМП является скачкообразным случайным процессом, при этом распределение времени пребывания ПМП в каждом состоянии не обязательно является экспоненциальным.

Примечание — Для ПМП характерно то, что процесс мгновенных вероятностных переходов представляет собой вложенную цепь Маркова.

Полумарковский процесс представляют в виде ориентированного графа (рисунок Д.5).

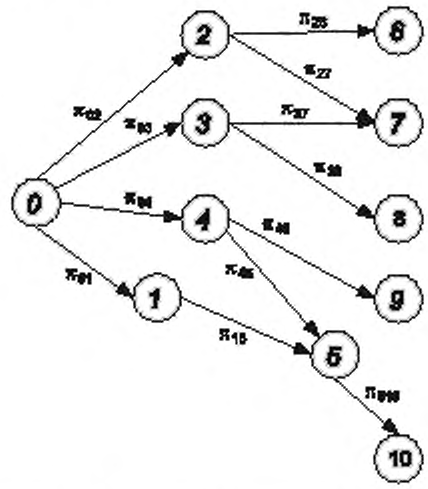


Рисунок Д.5 — Пример графа состояний и переходов полумарковского процесса

ПМП задают одним из следующих способов:

- начальным распределением $p = \{p_i, i \in I\}$, с использованием которого выбирается исходное состояние i, и связанной с ПМП матрицей $Q(t)$, элементы которой удовлетворяют следующим условиям:

а) $q_{ij}(t) \equiv 0$, если $t = 0$;

б) $q_{ij}(t)$ — неубывающие, непрерывные справа функции для $t \geq 0$,

в) $\sum_{j \in I} q_{ij}(t) = F_i \leq 1$ — функция распределения времени пребывания процесса в состоянии i;

- начальным распределением $p = \{p_i, i \in I\}$, матрицей переходных вероятностей вложенной цепи Маркова $\{\pi_{ij}, i, j \in I\}$ и матрицей функции распределения $\{F_{ij}(t), i, j \in I\}$ времени пребывания процесса в состоянии i при условии, что переход осуществляется в состояние j;

- начальным распределением $p = \{p_i, i \in I\}$ множеством функций распределения $\{F_i(t), i \in I\}$ времени пребывания и матрицей $Q(t)$ с элементами $q_{ij}(t)$ условных вероятностей того, что ПМП $\xi(t)$ попадет в состояние j, пробыв в состоянии i время не более t.

В качестве примера ниже приведены применяемые на практике представления элементов матриц $Q(t)$, связанных с ПМП:

$$q_{ij}(t) = \pi_{ij},\ t \geq 0,\ \sum_{j \in I} \pi_{ij} = 1,\ i, j \in I; \tag{Д.28}$$

$$q_{ij}(t) = \pi_{ij} \cdot \left[1 - \exp(-\lambda_i \cdot t)\right],\ t \geq 0,\ \sum_{j \in I} \pi_{ij} = 1,\ i, j \in I;\ \lambda_i > 0; \tag{Д.29}$$

$$q_{ij}(t) = \pi_{ij} \cdot F_j(t),\ t \geq 0,\ \sum_{j \in I} \pi_{ij} = 1,\ i, j \in I. \tag{Д.30}$$

С использованием матрицы $Q(t)$ определяют переходные вероятности $F_{ij}(t)$ (т. е. вероятности перехода из состояния i в состояние j за время t) путем решения системы интегро-дифференциальных уравнений следующего вида:

$$F_{ij}(t) = \left(1 - P_i(t)\right) \cdot \delta_{ij} + \sum_{k \in I} \int_0^t q'_{ik}(x) \cdot F_{kj}(t - x) \cdot dx,\ k, i, j \in I,\ t > 0, \tag{Д.31}$$

где $q'_{ik}(x)$ — производная от элемента $q_{ij}(t)$ матрицы $Q(t)$;

$P_i(t)$ — вероятность того, что ПМП не покинет к моменту времени t состояния i;

δ_{ij} — символ Кронекера, $\delta_{ij} = \begin{cases} 1 \text{ при } i = j; \\ 0 \text{ при } i \neq j. \end{cases}$

Если определить среднее время пребывания в состоянии i при условии, что после его окончания процесс перейдет в состояние j, через θ_{ij}, то среднее время θ_i пребывания ПМП в состоянии i вычисляют из соотношения:

$$\theta_i = \sum_{j \in I} \theta_{ij}, \qquad (Д.32)$$

а переходные вероятности π_{ij} — по формуле

$$\pi_{ij} = \theta_{ij} / \theta_i = \theta_{ij} / \sum_{j \in I} \theta_{ij}, \ i, j \in I. \qquad (Д.33)$$

Д.3.7 Пример Д.4. Пусть при анализе угроз безопасности информации в системе в соответствии с [10]—[12] необходимо рассчитать вероятность реализации угрозы несанкционированного доступа к файлу с конфиденциальной информацией одним из следующих двух способов: путем повышения привилегий (1-й способ) или путем изменения учетных записей (2-й способ).

Возможно следующее решение для примера Д.4.

Оба практических способа 1 и 2 основаны на внедрении соответствующих вредоносных программ. В этих условиях для моделирования применим аппарат ПМП. Граф соответствующего полумарковского процесса с двумя способами формального представления реализации угрозы несанкционированного доступа к файлам с защищаемой информацией приведен на рисунке Д.6.

На графе используются следующие обозначения. Цифрами в кружках обозначены номера состояния процесса:

0 — запущен процесс внедрения вредоносных программ или для изменения учетных записей, или для повышения привилегий с несанкционированным использованием системных функций;

1 — внедрена вредоносная программа для изменения учетных записей и запущена на выполнение, изменена учетная запись, созданы условия для проникновения к файлу с конфиденциальной информацией, начата попытка проникновения;

2 — получен доступ к файлу с конфиденциальной информацией, начато копирование файла в выбранную область памяти или на флэш-носитель;

3 — внедрена и запущена на выполнение вредоносная программа для повышения привилегий атакующего;

4 — повышены привилегии атакующего, начата попытка проникновения;

5 — получен доступ к файлу с конфиденциальной информацией, файл скопирован в выбранную область памяти или на флэш-носитель, угроза реализована.

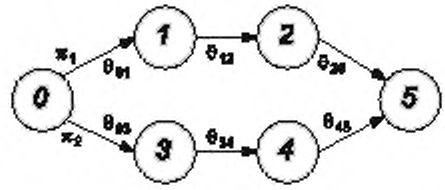


Рисунок Д.6 — Граф полумарковского процесса при формальном представлении реализации угрозы несанкционированного доступа к файлам с защищаемой информацией

Время θ_{ij} соответствует среднему значению времени перехода процесса из состояния i в состояние j, а π_1 и π_2 — вероятностям применения первого и второго способов соответственно.

В предположении, что время пребывания в i-м состоянии распределено экспоненциально, плотность распределения времени перехода в состояние j определяют в виде

$$f_{ij}(t) = (1/\theta_{ij}) \cdot \exp(-t/\theta_{ij}), \qquad (Д.34)$$

при этом $\theta_{01} = \theta_{12} = \theta_{25} = \theta_1$ и $\theta_{03} = \theta_{34} = \theta_{45} = \theta_2$.

Из формулы (Д.31) плотность распределения вероятности перехода процесса из нулевого состояния в конечное состояние (состояние 5) представляет собой свертку плотностей распределения вероятностей переходов из состояния в состояние по траекториям перемещения, соответствующим первому и второму способам доступа:

$f_{05}^{(1)}(t) = f_{01}(t) * f_{12}(t) * f_{25}(t)$ ***— для первого способа несанкционированного доступа;***

$f_{05}^{(2)}(t) = f_{03}(t) * f_{34}(t) * f_{45}(t)$ ***— для второго способа несанкционированного доступа.***

Здесь знак * обозначает операцию свертки.

При экспоненциальной аппроксимации распределений вероятностей следует

$$f_{05}^{(1)}(t) = \frac{1}{2}\cdot\left(t^2/\theta_1^3\right)\cdot\exp\left(-t/\theta_1\right),\ f_{05}^{(2)}(t) = \frac{1}{2}\cdot\left(t^2/\theta_2^3\right)\cdot\exp\left(-t/\theta_2\right). \quad \text{(Д.35)}$$

Вероятность того, что за время t процесс достигнет конечного состояния, т. е. перейдет из состояния 0 в состояние 5 и тем самым угроза безопасности информации будет реализована, определяется из соотношения

$$P_u(t) = F_{05}(t) = \pi_1\cdot\int_0^t f_{05}^{(1)}(x)dx + \pi_2\cdot\int_0^t f_{05}^{(2)}(x)\cdot dx. \quad \text{(Д.36)}$$

С учетом того, что $\pi_1 + \pi_2 = 1$,

$$P_u(t) = 1 - \pi_1\cdot\exp(-t/\theta_1)\cdot[t^2/(2\cdot\theta_1^2) + t/\theta_1 + 1] - (1-\pi_1)\cdot\exp(-t/\theta_2)\cdot[t^2/(2\cdot\theta_2^2) + t/\theta_2 + 1]. \quad \text{(Д.37)}$$

График расчетной зависимости для выбранных значений средних времен выполнения соответствующих процессов приведен на рисунке Д.7.

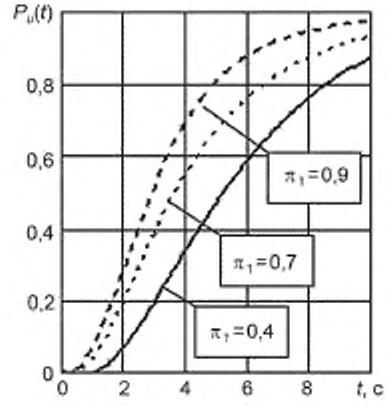


Рисунок Д.7 — График зависимости вероятности достижения моделируемым процессом конечного состояния за время t при $\theta_1 = 1$с, $\theta_2 = 2$с

Системный анализ расчетов показал, что без применения мер защиты угроза несанкционированного доступа одним из рассматриваемых способов с высокой вероятностью (выше 0,8) может быть реализована за единицы секунд.

Д.3.8 Более широкими возможностями для моделирования угроз безопасности информации обладает аппарат составных сетей Петри—Маркова (СПМ) с логическими условиями выполнения моделируемого процесса. Логические условия определяют правила срабатывания специально вводимых в СПМ логических переходов.

Краткая характеристика таких сетей сводится к следующему.

Пусть моделируемый процесс состоит из нескольких подпроцессов, каждый из которых происходит или между начальной позицией и логическим переходом, или между двумя логическими переходами, или между логическим переходом и конечной позицией процесса. Такие СПМ названы составными. Как и традиционные СПМ, составные сети представляются в виде ориентированного графа (см. рисунок Д.8), в котором кружки (позиции) означают состояния моделируемого процесса, вертикальные или горизонтальные черты — переходы процесса между состояниями, а дуги — направления перемещения процесса из состояния (или состояний) в переход или из перехода в состояния.

Каждому логическому переходу поставлена в соответствие определенная пропозиционная логика срабатывания. Перемещение подпроцесса по состояниям может происходить по нескольким траекториям, время перемещения из состояния в переход в общем случае является конечным и случайным. При этом принято допущение, что перемещение из перехода в состояние происходит мгновенно (поскольку на практике это время на порядки меньше времени перемещения из состояния в переход).

Для обозначения перемещения процесса по СПМ используют метки (как и в сетях Петри), при этом позиции в зависимости от состояния процесса, разделяются на помеченные и непомеченные. Множество помеченных позиций называют разметкой СПМ. Разметка может быть начальной (0-разметка) и текущей (*л*-разметка), при этом 0-разметка формируется при старте процесса, а *л*-разметка — после *л* шагов процесса.

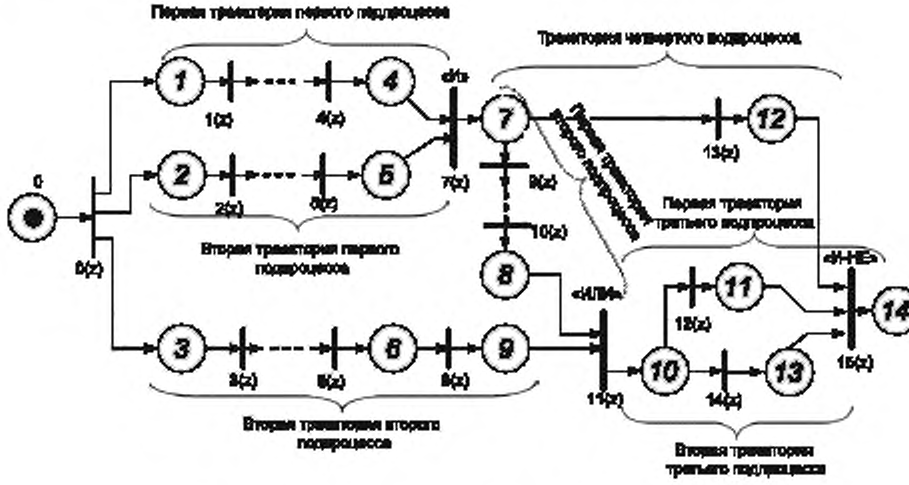


Рисунок Д.8 — Пример графа составной сети Петри—Маркова

Примечание — В общем случае может быть определена любая логика срабатывания логического перехода. Это значительно расширяет возможности моделирования в отличие от классических сетей Петри-Маркова, когда переходы срабатывают только тогда, когда для каждой входящей в переход дуги имеется не менее одной метки в инцидентной позиции (на практике метки могут именоваться маркерами или фишками).

При построении графа составной СПМ следует соблюдать следующие правила:

- СПМ должна начинаться с одной или нескольких начальных позиций и заканчиваться конечной позицией;
- должна быть установлена начальная разметка сети;
- в сети не может быть две подряд позиции или два подряд перехода;
- в сети могут применяться кратные дуги, но тогда в состоянии, из которого они исходят, должно находиться или накапливаться такое же или большее количество маркеров к переходам, в которые входят кратные дуги, должны быть сопоставлены соответствующие правила срабатывания;
- из перехода СПМ может исходить несколько дуг, при этом если в переход поступил один маркер, то по всем исходящим из него дугам выходит по одному маркеру;
- для логического перехода характерно то, что он всегда имеет две и более входящих дуг;
- в СПМ могут иметь место тупиковые позиции, в которых развитие процесса прекращается (например, для того чтобы показать, где может остановиться процесс, не достигнув конечной позиции);
- наличие нескольких траекторий, которые выходят из одной позиции, свидетельствуют о том, что моделируемый подпроцесс является полумарковским и для него используется аппарат, характеристика которого представлена в Д.3.6;
- на графе СПМ переходы обозначаются номером с буквой *z*, а позиции просто нумеруются, в индексах функций и параметров (например, для вероятностей выбора пути развития процесса) первая цифра означает номер состояния, из которого исходит дуга, а вторая через запятую — номер перехода, в который она входит.

Каждый подпроцесс, т. е. перемещение моделируемого процесса по одной из траекторий, является марковским процессом, при этом время перемещения по траектории рассчитывается как сумма случайных времен перемещения из позиций в переходы. Например, между двумя логическими переходами по траектории имеется *N* позиций и переходов (см. рисунок Д.9), в общем случае по каждой из дуг, входящих в переход, процесс перемещается за конечное случайное время. Тогда среднее время перемещения подпроцесса из позиции 0 в переход *N*(*z*) по рассматриваемой траектории представляет собой сумму средних значений независимых случайных величин:

$$\tau_{\Sigma} = \sum_{n=1}^{N} \tau_{n-1,\ n},\ n = \overline{1,\ N}. \qquad (Д.38)$$

В логическом переходе могут сходиться или две и более траекторий одного подпроцесса, или два и более подпроцессов. С учетом времен перемещения, входящих в логический переход подпроцессов, рассчитывается среднее время срабатывания логического перехода.

В таблице Д.1 приведены соотношения для расчета времен срабатывания наиболее широко используемых в моделировании реализации угроз безопасности информации логических переходов.

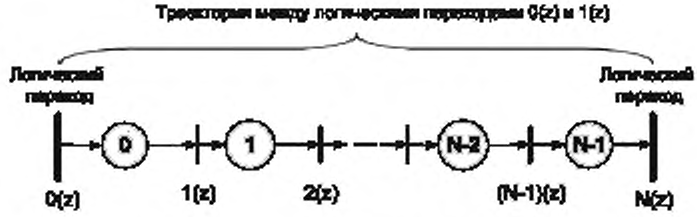


Рисунок Д.9 — Траектория перемещения подпроцесса по сети Петри—Маркова по одной из траекторий между двумя логическими переходами

Таблица Д.1 — Соотношения для расчета среднего времени срабатывания переходов

Логическое условие	Соотношение для расчета среднего времени срабатывания перехода	Объяснение логики действия
$A \cap B$	Для двух входящих дуг $\tau_{И}^{(2)} = \frac{\tau_1^2 + \tau_1 \cdot \tau_2 + \tau_2^2}{\tau_1 + \tau_2}$; для трех входящих дуг $\tau_{И}^{(3)} = \tau_1 + \tau_2 + \tau_3 - \left(\frac{\tau_1 \cdot \tau_2}{\tau_1 + \tau_2} + \frac{\tau_1 \cdot \tau_3}{\tau_1 + \tau_3} + \frac{\tau_2 \cdot \tau_3}{\tau_2 + \tau_3}\right) +$ $+ \frac{\tau_1 \cdot \tau_2 \cdot \tau_3}{\tau_1 \cdot \tau_2 + \tau_1 \cdot \tau_3 + \tau_2 \cdot \tau_3}$	Логика «И»: процесс приходит к переходу по всем дугам; τ_1, τ_2, τ_3 — средние времена на логический переход по дугам 1, 2 и 3 соответственно
$A \cup B$	Для двух входящих дуг $\tau_{или}^{(2)} = \frac{\tau_1 \cdot \tau_2}{\tau_1 + \tau_2}$; для трех входящих дуг $\tau_{или}^{(3)} = \frac{\tau_1 \cdot \tau_2 \cdot \tau_3}{\tau_1 \cdot \tau_2 + \tau_1 \cdot \tau_3 + \tau_2 \cdot \tau_3}$	Логика «ИЛИ»: процесс приходит к переходу хотя бы по одной из дуг
$(A \cap B) \cup C$	Для трех входящих дуг $\tau_{и\text{-}или}^{(3)} = \frac{\tau_1 \cdot \tau_2}{\tau_1 + \tau_2} + \frac{\tau_1^2 \cdot \tau_3}{(\tau_1 + \tau_3)^2} + \frac{\tau_2^2 \cdot \tau_3}{(\tau_2 + \tau_3)^2} -$ $- \frac{\tau_1 \cdot \tau_2 \cdot \tau_3}{\tau_1 \cdot \tau_2 + \tau_1 \cdot \tau_3 + \tau_2 \cdot \tau_3}$	Логика «И-ИЛИ»: процесс приходит к переходу по первой (A) и второй (B) дугам или по третьей (C) дуге
$A \cap \bar{B}$	Для двух входящих дуг: $\tau_{и\text{-}не}^{(2)} = \tau_1 \cdot (1 + \tau_2 / \tau_1)$	Логика «И-НЕ»: процесс приходит к переходу по первой (A) дуге и не успевает прийти по второй дуге (B)
$(A \cap B) \cap \bar{C}$	Для трех входящих дуг: $\tau_{и\text{-}не}^{(3)} = \tau_{и\text{-}не}^{(2)} \cdot \left(1 + \frac{\tau_3}{\tau_{и\text{-}не}^{(2)}}\right)$	Логика «И-НЕ» для трех дуг: процесс приходит по первым двум (A и B) дугам и не успевает прийти по третьей дуге (C)
$A \cap B^*$	Для двух входящих дуг: $\tau_{И\&НБ}^{(2)} = \tau_1$. Обозначение (2) в верхнем индексе означает отношение к двум входящим дугам, обозначение «И&НБ» в нижнем индексе означает отношение к применяемой логике «И-НЕ(Блок)», связанной с отсутствием блокирования действий по второй дуге — см. объяснение в правой колонке этой строки	Логика «И-НЕ(Блок)»: для двух дуг: поток по первой дуге подошел к переходу (условие A) и поток по второй дуге не заблокирован с вероятностью $1 - P_{21}$ (условие B^*). Если процесс по второй дуге заблокирован, то блокируется срабатывание логического перехода независимо от выполнения условия A

Окончание таблицы Д.1

Логическое условие	Соотношение для расчета среднего времени срабатывания перехода	Объяснение логики действий
$(A \cap B) \cap C^{*}$	Для трех входящих дуг: $\tau^{(3)}_{\text{И\&НБ}} = \left(\tau_1^2 + \tau_1 \cdot \tau_2 + \tau_2^2\right) / (\tau_1 + \tau_2)$. Обозначение (3) в верхнем индексе означает отношение к трем входящим дугам, обозначение «И&НБ» в нижнем индексе означает отношение к применяемой логике «*И*-НЕ(Блок)», связанной с блокированием действий — см. объяснение в правой колонке этой строки	Логика «*И*-НЕ(Блок)» для трех дуг: потоки по первым двум дугам подошли к переходу (условия *A* и *B*) и по третьей дуге поток не заблокирован с вероятностью $1 - P_{31}$ (условие C^{*}). Если процесс по третьей дуге заблокирован, то блокируется срабатывание логического перехода независимо от выполнения условий *A* и *B*

С использованием соотношений из таблицы Д.1 могут быть рассчитаны общее среднее время реализации угрозы и вероятность ее реализации за заданное время.

Д.3.9 Пример Д.5. Пусть в модернизируемой системе, обеспечивающей деятельность коммерческого предприятия, в соответствии с требованиями ГОСТ Р 27002 оценивают риски реализации угроз. Установлено, что одной из таких угроз является запуск вредоносного скрипта, который может быть внедрен с использованием файла типа cookie с последующим копированием необходимой информации (файл типа cookie — это небольшой фрагмент данных, отправляемый web-сервером и хранимый на компьютере пользователя, используется для аутентификации пользователя, хранения персональных предпочтений и настроек пользователя, отслеживания состояния сеанса доступа пользователя, в переводе с английского «cookie» — «печенье»).

Требуется оценить риск реализации угрозы запуска вредоносного скрипта, внедряемого с использованием файла типа cookie.

Возможно следующее решение для примера Д.5.

На рисунке Д.10 приведена СПМ, описывающая в графическом виде процесс реализации угрозы копирования информации с использованием файла cookie в условиях отсутствия мер защиты.

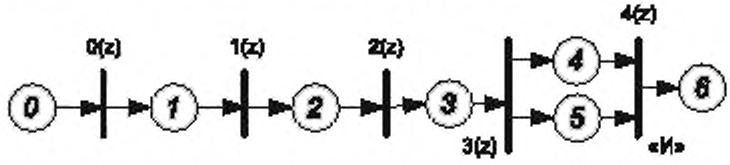


Рисунок Д.10 — Граф СПМ, описывающий процесс реализации угрозы для запуска вредоносного скрипта в условиях отсутствия мер защиты

На графе цифрами в кружках обозначены номера состояний процесса, цифрами с буквой z в скобках — номера переходов. Дополнительно использованы обозначения:

а) для состояний:

0 — начальное состояние процесса, нарушитель готов к проведению атаки внедрения скрипта. Атакуемый хост подготовил запрос на Web-сервер для поиска нужного ему информационного ресурса;

1 — Web-север получил запрос и подготовил к передаче на хост пользователя файла cookie;

2 — файл cookie перехвачен «сниффером» и передан на хост нарушителя (под «сниффером» понимается программа, способная перехватывать и анализировать трафик, проходящий через цифровую сеть);

3 — в файл cookie на хосте нарушителя внедрен вредоносный скрипт и файл передан на атакуемый хост;

4 — файл cookie принят web-браузером на атакуемом хосте, открыт и запущен вредоносный скрипт;

5 — на атакуемом хосте найден нужный нарушителю файл пользователя и подготовлен к передаче по сети;

6 — скопированный файл передан на хост нарушителя или на сетевой адрес, нужный нарушителю;

б) для переходов:

0(z) — передача запроса с атакуемого хоста на Web-сервер;

1(z) — передача Web-сервером файла cookie на хост пользователя;

2(z) — перехват файла cookie «сниффером», передача его на хост нарушителя и внедрение в него нужного нарушителю скрипта;

3(z) — передача файла cookie с внедренным скриптом на атакуемый хост и запуск скрипта;

4(z) — логический переход с логикой срабатывания «И», срабатывающий, если запущен вредоносный скрипт и завершено копирование файла пользователя, результатом срабатывания перехода является передача файла пользователя на хост нарушителя.

При экспоненциальной аппроксимации времени развития угрозы (до ее реализации) вероятность реализации угрозы рассчитывается по формуле

$$P_u(t) = 1 - \exp\left(-\frac{t}{\tau_u^{(0)}}\right), \quad (Д.39)$$

где $\tau_u^{(0)} = \tau_{0,0} + \tau_{1,1} + \tau_{2,2} + \tau_{3,3} + \tau_{\text{"И"}}$;

$\tau_{\text{"И"}}$ — *среднее время срабатывания логического перехода 4(Z) с логикой «И», рассчитываемое согласно таблице 1 по формуле*

$$\tau_{\text{"И"}} = (\tau_{5,4}^2 + \tau_{5,4} \cdot \tau_{4,4} + \tau_{4,4}^2)/(\tau_{5,4} + \tau_{4,4}). \quad (Д.40)$$

Примечание — Время $\tau_{0,0}$ *является величиной, обратной интенсивности возникновения угроз, и может составлять от единиц минут до нескольких суток.*

СПМ, описывающая в графическом виде реализацию угрозы копирования информации с использованием файла cookie для запуска вредоносного скрипта в условиях применения меры ЗИ, приведена на рисунке Д.11.

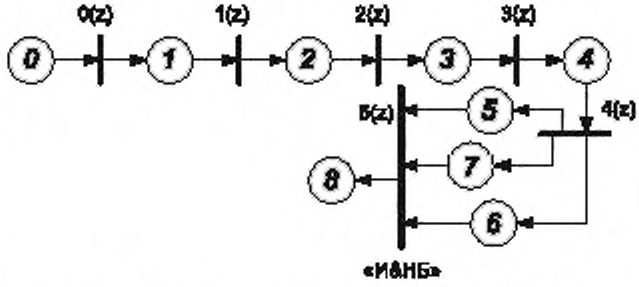


Рисунок Д.11 — Граф СПМ, описывающий процесс реализации угрозы в условиях применения специальной программы обнаружения вредоносного скрипта

При этом вероятность реализации угрозы рассчитывают по формуле

$$P_u(t) = P_{\text{обн}} \cdot \left[1 - \exp\left(-t / \tau_u^{(\text{ЗИ})}\right)\right], \quad (Д.41)$$

где $\tau_u^{(\text{ЗИ})} = \tau_{0,0} + \tau_{1,1} + \tau_{2,2} + \tau_{3,3} + \tau_{\text{"И\&НБ"}}$;

$\tau_{\text{"И\&НБ"}}$ — *среднее время срабатывания логического перехода 5(z) с логикой «И», рассчитываемое в соответствии с таблицей 1 (нижняя строка),*

$$\tau_{\text{"И\&НБ"}}^{(3)} = \tau_{5,5}^2 \left(\tau_{5,5}^2 + \tau_{5,5} \cdot \tau_{7,5} + \tau_{7,5}^2\right) / \left(\tau_{5,5} + \tau_{7,5}\right); \quad (Д.42)$$

$P_{\text{обн}}$ — *вероятность обнаружения вредоносного скрипта программой «cookie-менеджер».*

На графе рисунка Д.11 использованы следующие обозначения:

а) для состояний:

0 — начальное состояние процесса, нарушитель готов к проведению атаки внедрения скрипта. Атакуемый хост подготовил запрос на Web-сервер для поиска нужного ему информационного ресурса;

1 — Web-север получил запрос и подготовил к передаче на хост пользователя файла cookie;

2 — файл cookie перехвачен «сниффером» и передан на хост нарушителя;

3 — в файл cookie на хосте нарушителя внедрен вредоносный скрипт и файл подготовлен к передаче на атакуемый хост;

4 — файл cookie принят web-браузером на атакуемом хосте для выполнения;

5 — на атакуемом хосте найден нужный нарушителю файл пользователя, скопирован и подготовлен к передаче по сети;

6 — запущена программа «cookie-менеджер», обнаруживающая с вероятностью P_{det} *подлежащий выполнению скрипт;*

7 — подана команда на запуск вредоносного скрипта;

8 — скопированный файл пользователя передан на хост нарушителя или на сетевой адрес, нужный нарушителю;

б) для переходов:

0(z) — передача запроса с атакуемого сервера на Web-сервер;

1(z) — передача Web-сервером файла cookie на хост пользователя;

2(z) — перехват файла cookie «сниффером», передача его на хост нарушителя и внедрение в него нужного нарушителю скрипта;

3(z) — передача файла cookie с внедренным скриптом на атакуемый хост;

4(z) — запуск вредоносного скрипта;

5(z) — логический переход, срабатывающий, если запущен вредоносный скрипт, завершено копирование файла пользователя и не обнаружен к этому моменту времени вредоносный скрипт, результатом срабатывания перехода является передача файла пользователя на хост нарушителя — реализация угрозы.

Пусть в рамках примера принято допущение $\tau_{0,0} \approx \tau_{1,1} \approx \tau_{2,2} \approx \tau_{3,3} \approx \tau_{4,4} \approx \tau_{5,5} \approx \tau_{6,5} \approx \tau_{7,5} = \tau$. *Тогда среднее время срабатывания логического перехода 4(z) на рисунке Д.10 в соответствии с формулой (Д.40) равно* $\tau_{\text{"И"}} = 5{,}5 \cdot \tau$, *а среднее время срабатывания логического перехода 5(z) на рисунке Д.11 в соответствии с формулой (Д.42) равно* $\tau^{(3)}_{\text{"И\&НБ"}} = 6{,}5 \cdot \tau$. *Вероятности реализации угроз для условий без применения и при применении меры защиты оцениваются соответственно по следующим формулам:*

$$P_u(t) = 1 - \exp[-t/(5{,}5 \cdot \tau)]; \quad \text{(Д.43)}$$

$$P_u(t) = (1 - P_{\text{обн}}) \cdot \{1 - \exp[-t/(6{,}5 \cdot \tau)]\}. \quad \text{(Д.44)}$$

На рисунке Д.12 приведены зависимости вероятности реализации угрозы от соотношения t/τ *для условия отсутствия (т. е. без применения) и при условии применения программы обнаружения вредоносных скриптов «cookie-менеджер», рассчитанные по формулам (Д.43)—(Д.44) при условных вероятностях обнаружения угроз* $P_{\text{обн}}$ *на уровнях 0,1, 0,5, 0,9.*

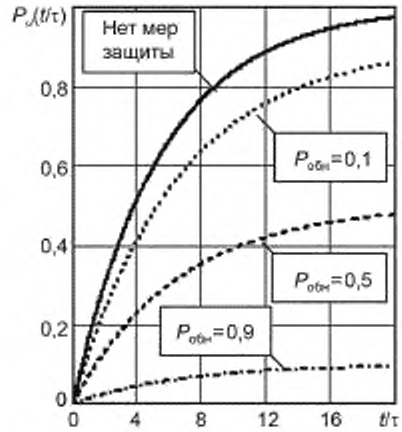


Рисунок Д.12 — Зависимости вероятности реализации угрозы от соотношения t/τ *для условия отсутствия меры защиты информации и в условиях ее применения*

Системный анализ результатов расчетов показал, что с увеличением вероятности обнаружения вредоносных скриптов возможность реализации угроз существенно падает.

Сравнение вероятностей реализации угрозы для условия отсутствия меры ЗИ и при условии ее применения позволяет оценить эффективность (см. приложение Е) и обосновать целесообразность применения рассмотренной меры ЗИ в системе.

Д.4 Балльные методы оценки рисков нарушения безопасности системы

Д.4.1 В случае, когда статистических данных для рисков реализации угроз недостаточно (включая оценку возможного ущерба) или невозможен учет некоторых важных факторов аналитическими методами, применяют балльные методы оценки — см., например ГОСТ Р ИСО/МЭК 27002. При использовании балльных методов строят шкалу оценок в табличной или графической форме. При этом в качестве возможных видов ущербов могут быть, например, рассмотрены:

- ущерб репутации организации;
- ущерб, связанный с нарушением действующего законодательства;
- ущерб для здоровья персонала;
- экологический ущерб;
- ущерб, связанный с разглашением персональных данных;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов.

Далее формируют балльные шкалы оценки ущерба. Пример формирования шкалы оценок в интервале значений 0—10 приведен в таблице Д.2. Затем баллы по результатам оценки различных видов ущерба суммируются и переводятся в качественные суждения о размерах возможного ущерба по табличной шкале — см. примерный вариант в таблице Д.3.

Таблица Д.2 — Вариант формирования шкалы оценки ущерба (пример)

Вид ущерба	Величина ущерба, соответствующая оценке в баллах				
	2 балла	4 балла	6 баллов	8 баллов	10 баллов
Ущерб репутации организации	Негативная реакция отдельных чиновников, общественных деятелей	Критика в СМИ, не получившая широкого общественного резонанса	Негативная реакция членов законодательных органов власти	Критика в СМИ с последствиями в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок	Негативная реакция на уровне руководства государства
Ущерб для здоровья персонала	Минимальный ущерб, не связанный с госпитализацией или длительным лечением	Средний ущерб, связанный с лечением одного или нескольких сотрудников при отсутствии длительных отрицательных последствий	Серьезные последствия (продолжительная госпитализация, инвалидность одного или нескольких сотрудников)	—	Гибель людей
Финансовые потери, связанные с восстановлением ресурсов	Менее 1000 у.е.		От 1000 у.е. до 10000 у.е.	От 10000 у.е. до 100000 у.е.	Свыше 100000 у.е.
Дезорганизация деятельности в связи с недоступностью данных	До 15 минут	От 15 минут до 1 часа	От 1 часа до 3 часов	От 3 часов до 1 суток	Более 1 суток
...	...	...			

Таблица Д.3 — Пример соответствия балльной оценки и качественного суждения о размере ущерба от реализации угрозы

Размер ущерба в баллах	Показатель качественной оценки размера ущерба	Трактовка качественной оценки размера ущерба
9 и менее	Н (незначительный)	Ущербом можно пренебречь
10—19	М (малый)	Последствия легко устранимы, с малыми затратами на ликвидацию
20—29	С (средний)	Последствия умеренны, не связаны с крупными затратами, не затрагивают критически важные задачи
30—39	Б (большой)	Серьезные последствия со значительными затратами, влияющими на выполнение критически важных задач
Более 40	К (критический)	Невозможно решение критически важных задач

Балльные оценки возможного ущерба могут оцениваться также по графической шкале, например, с использованием полярной шкалы, на которой устанавливают крайние противоположные (полярные) результаты оценки ущерба — «отсутствие ущерба» и «неприемлемый ущерб». На таких шкалах могут рассматриваться несколько типов оценок: точечные количественные, интервальные, вербальные (описательные), при этом могут применяться метрические или порядковые шкалы.

В качестве максимального значения на шкале устанавливается точка справа, соответствующая неприемлемому ущербу, а в качестве минимального — точка слева, соответствующая отсутствию ущерба, что позволяет построить метрическую шкалу для оценки ущербов от реализации угроз безопасности информации для системы.

Особенность такой шкалы заключается в некоторой ее универсальности относительно видов ущерба. Шкалы для разнородных ущербов могут быть сведены к единой шкале оценок. Для этого первоначально в качестве базовой берется вербальная полярная шкала. Наиболее часто при построении такой шкалы используют шесть градаций оценок — см. рисунок Д.13.

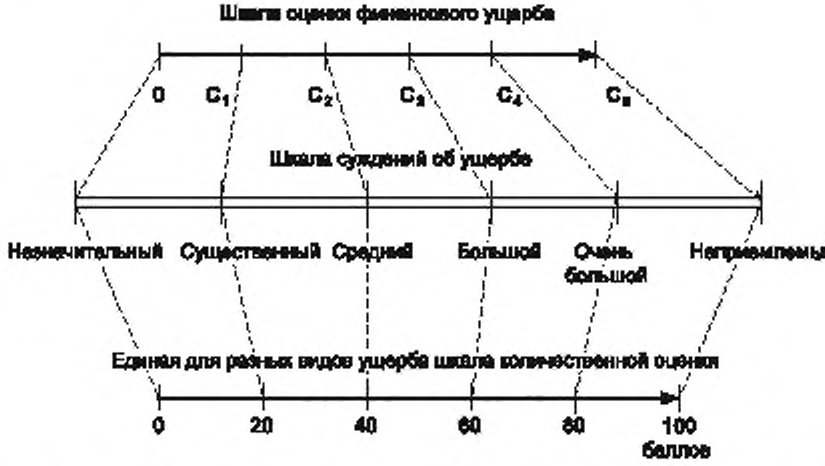


Рисунок Д.13 — Возможный вариант единой количественной шкалы оценок ущерба и приведения к ней шкал разнородных ущербов

Если имеется единая количественная шкала, то для приведения к ней оценок величин ущербов необходимо нормировать их по единой шкале относительно неприемлемого ущерба. В этом случае берется отношение оцениваемого φ-го вида ущерба $c^{(\varphi)}$ к его неприемлемому значению $c_{\max}^{(\varphi)}$. Такое отношение β_Φ называют индексом ущерба от реализации угрозы (далее индекс ущерба):

$$\beta_\varphi = c^{(\varphi)} / c_{\max}^{(\varphi)}; \qquad (Д.45)$$

Если ущерб оценивается по вербальной шкале, то на ней определяется точка предельного ущерба справа и все ущербы выше этой точки рассматриваются как неприемлемые. Точке неприемлемого ущерба ставится в соответствие верхняя граница единой числовой шкалы и затем по ней определяется индекс данного вида ущерба β_φ с учетом важности вида ущерба

$$\beta_\Phi = \sum_{\varphi \in \Phi} V_\varphi \cdot \beta_\varphi, \qquad (Д.46)$$

где V_φ — коэффициент важности φ-го вида ущерба, при этом $\sum_{\varphi \in \Phi} V_\varphi = 1$.

Балльные методы могут применяться также для оценки возможностей реализации угроз безопасности информации в системе. При этом используют табличные шкалы, в которых за основу берутся экспертные суждения специалистов о возможности реализации каждой из угроз в данной системе. Вариант такой шкалы, построенной по аналогии с табличной шкалой оценки ущербов, приведен в таблице Д.4.

Уровень существенности угрозы может быть оценен экспертно на основе проведенных оценок ущерба и возможности реализации угрозы. А затем балльные оценки переводятся в качественные суждения о существенности угрозы — см. возможные варианты (примеры) в таблицах Д.5 и Д.6.

Таблица Д.4 — Вариант соответствия балльной оценки и качественного суждения о возможности реализации угрозы безопасности информации

Оценка в баллах	Качественная оценка возможности реализации угрозы	Трактовка качественной оценки вероятности реализации угрозы
9 и менее	М (маловероятна)	Реализация угрозы маловероятна
10—19	Н (низкая)	Вероятность реализации угрозы низкая
20—29	С (средняя)	Вероятность реализации угрозы средняя
30—39	В (высокая)	Реализация угрозы вполне вероятна
Более 40	Д (очень высокая)	Реализация угрозы неизбежна

Таблица Д.5 — Вариант балльной шкалы оценки степени нарушения безопасности системы

Размер ущерба	Оценка степени реализации угрозы				
	М	Н	С	В	Д
НЗ (незначительный)	1	2	2	3	6
Н (низкий)	2	2	3	4	7
С (средний)	3	4	5	6	8
Б (большой)	4	5	6	8	9
К (критический)	5	6	7	9	10

Таблица Д.6 — Вариант соответствия балльной оценки и качественного суждения о существенности угрозы безопасности системы

Оценка степени нарушения безопасности системы в баллах	Интерпретация оценки степени нарушения безопасности системы в вербальной шкале
1 балл и менее	Очень низкий риск
2—3 балла	Низкий риск
4—6 баллов	Средний риск
7—9 баллов	Высокий риск
10 баллов	Недопустимый риск

Примечание — По соглашению заинтересованных сторон устанавливают уровень допустимой степени нарушения безопасности системы в баллах. Например, если экспертная оценка степени нарушения безопасности составляет 3 и более баллов, то угроза может быть охарактеризована как «существенная».

Тем самым балльный метод может быть использован для обоснования перечня существенных угроз (см. таблицу Д.5, где закрашенные ячейки соответствуют таким угрозам).

Д.4.2 Пример Д.6. Пусть некоторое областное Главное управление здравоохранения оснащается специализированной автоматизированной информационной системой. В ней предстоит обрабатывать защищаемую информацию, включающую:

- персональные данные о сотрудниках, содержащиеся в базе данных;

- служебную информацию, содержащую сведения о деятельности учреждения, а также сведения бухгалтерской и финансовой отчетности.

Эта информация может быть передана как внутри управления по системе, так в другие системы управления, перенесена персоналом с применением отчуждаемых носителей, а также передана другим инстанциям через сеть Интернет.

Требуется определить существенные угрозы для рассматриваемой системы.

Возможно следующее решение для примера Д.5.

Для оценки риска реализации возможных угроз безопасности информации в системе и определения существенных угроз применяют экспертный балльный метод. В результате анализа экспертами установлено, что источниками угроз безопасности информации в системе могут быть:

- внешний и внутренний нарушитель;

- программно-аппаратная закладка;

- носитель вредоносной программы (флэш-память, CD-диск).

Внешними нарушителями могут быть представители криминальных структур, представители вышестоящих и нижестоящих организаций, недобросовестные партнеры, посторонние лица. Внешний нарушитель имеет следующие возможности:

- осуществлять удаленный несанкционированный доступ к защищаемой информации через сеть Интернет, ее копирование или уничтожение;

- инфицировать систему вредоносными программами, позволяющими вывести ее из строя или копировать и передавать через сеть Интернет по заданному нарушителем сетевому адресу нужную ему информацию.

К основным внутренним нарушителям относятся:

- лица, имеющие санкционированный доступ на территорию управления, но не имеющие доступа к информационным ресурсам (охранники, энергетики, сантехники, уборщицы и другие должностные лица, обеспечивающие нормальное функционирование защищаемого объекта);

- зарегистрированные пользователи системы, осуществляющие доступ к ее ресурсам с рабочих мест, в т. ч. системные администраторы;

- посторонние лица, приходящие в управление к его сотрудникам по личным вопросам или в интересах их решения в служебном порядке.

- программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие поставку, сопровождение и ремонт технических средств в составе системы.

Эти нарушители могут:

- осуществить несанкционированный доступ к защищаемой информации через автоматизированные рабочие места пользователей или через серверы системы, ее копирование или уничтожение;

- нарушить функционирования системы путем уничтожения или модификации системной информации (например, системных файлов операционной системы) или файлов и программных модулей системы управления базой данных (например, путем уничтожения или модификации индексных файлов в базе данных);

- внедрить программно-аппаратные и программные закладки в поставляемое оборудование и прикладные программы или инсталлировать вредоносные программы, реализующие весь спектр угроз относительно защищаемой информации в системе;

- непреднамеренно уничтожить файлы защищаемой информации или инфицировать систему вредоносными программами при неконтролируемом использовании личных носителей информации.

Наибольшими возможностями по реализации угроз безопасности обладают программисты — разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие поставку, сопровождение и ремонт технических средств автоматизированной информационной системы.

Согласно принятой модели угроз безопасности информации выделены угрозы удаленного несанкционированного доступа из сети Интернет и угрозы непосредственного несанкционированного доступа.

Угрозы удаленного несанкционированного доступа из сети Интернет в операционную среду автоматизированной информационной системы с возможным инфицированием вредоносной программой характеризуются потенциальными возможностями:

- копирования персональных данных, хранящихся в электронной базе данных управления;

- модификации или уничтожения персональных данных, хранящихся в электронной базе данных управления;

- блокирования использования базы данных управления (например, путем уничтожения или модификации программ в составе системы управления базой данных, уничтожения индексных файлов);

- копирования, уничтожения или модификации файлов со служебной информацией и содержащих сведения бухгалтерской и финансовой отчетности;

- несанкционированной записи в базу данных сведений о новых физических лицах.

Угрозы непосредственного несанкционированного доступа характеризуются последующей реализацией тех же действий, что и при удаленном доступе, и дополнительно:

- внедрением программно-аппаратных закладок в оборудование системы, а также программных закладок в поставляемое системное и прикладное программное обеспечение;

- несанкционированной передачей во внешнюю сеть служебной информации и сведений бухгалтерской и финансовой отчетности;

- непреднамеренным уничтожением записей в базе данных или исполняемых файлов, перемещением файлов в иные каталоги и директории.

Возможные результаты оценки ожидаемых ущербов при реализации каждой из угроз, входящих в указанный перечень, приведены в таблице Д.7.

Таблица Д.7 — Результаты экспертной оценки

Наименование обобщенных угроз	Оценка ущерба от реализации угрозы	Оценка возможности реализации угрозы	Решение о существенности угрозы
Копирование внешним нарушителем персональных данных, хранящихся в электронной базе данных	Незначительный	Маловероятная	Несущественная
Копирование внутренним нарушителем персональных данных, хранящихся в электронной базе данных	Низкий	Низкая	Существенная
Модификация или уничтожение внешним нарушителем персональных данных, хранящихся в электронной базе данных	Низкий	Низкая	Несущественная
Модификация или уничтожение внутренним нарушителем персональных данных, хранящихся в электронной базе данных	Низкий	Высокая	Существенная
Блокирование внешним нарушителем использования базы данных путем уничтожения или модификации программ в составе системы управления базой данных, уничтожения индексных файлов	Средний	Средняя	Существенная
Блокирование внутренним нарушителем использования базы данных путем уничтожения или модификации программ в составе системы управления базой данных, уничтожения индексных файлов	Средняя	Высокая	Существенная
Копирование внешним нарушителем файлов со служебной информацией или содержащих сведения бухгалтерской и финансовой отчетности	Низкий	Высокая	Существенная
Копирование внутренним нарушителем файлов со служебной информацией или содержащих сведения бухгалтерской и финансовой отчетности	Низкий	Высокая	Существенная
Уничтожение или модификация внешним нарушителем файлов со служебной информацией и содержащих сведения бухгалтерской и финансовой отчетности	Низкий	Низкая	Несущественная
Уничтожение или модификация внутренним нарушителем файлов со служебной информацией или содержащих сведения бухгалтерской и финансовой отчетности	Низкий	Низкая	Несущественная
Внедрение внутренним нарушителем программно-аппаратных и программных закладок или инфицирование системы вредоносной программой с последующим выполнением любого из указанных ранее несанкционированных действий	Низкий	Высокая	Существенная
Непреднамеренное уничтожение записей в базе данных или исполняемых файлов, перемещения файлов в иные каталоги и директории	Низкий	Высокая	Существенная

В итоге содержимое таблицы Д.7 характеризует результаты экспертной оценки для примера Д.6.

Приложение Е
(справочное)

Методы определения допустимых значений рисков

Е.1 Общие положения

Е.1.1 В процессе определения системных требований предельно допустимые значения рисков устанавливают в качестве условной границы нормы для максимального значения вероятности реализации существенных угроз. Превышение этой границы считают недопустимым. Сами допустимые значения рисков используют при решении задач системного анализа — см. раздел 7 и ГОСТ Р 59349.

Е.1.2 Предельно допустимые значение оценивают и устанавливают:

- для риска нарушения функционирования системы (например, в результате преднамеренного воздействия на общесистемное программное или программно-аппаратное обеспечение и прикладные программы и пользовательскую информацию, в результате которого система переходит в состояние «Отказ в обслуживании»);
- для риска утечки пользовательской информации, циркулирующей в системе и не подлежащей распространению в соответствии с установленными требованиями заинтересованных сторон системы;
- для риска нарушения надежности реализации процесса определения системных требований в части ЗИ.

Примечание — Предельно допустимое значение риска нарушения функционирования системы из-за преднамеренного воздействия на общесистемное программное, программно-аппаратное обеспечение или на пользовательскую информацию определяют для стадии эксплуатации системы. При этом по согласованию заинтересованных сторон задается значение допустимой вероятности реализации существенной угрозы при каждой попытке такой реализации. В ходе определения указанных допустимых значений могут учитываться допустимые размеры риска выхода из строя программного и аппаратного обеспечения, обусловленного его ненадежностью и оцениваемого требуемыми значениями вероятности безотказной работы систем, например, в соответствии с ГОСТ Р 27.003 и ГОСТ Р 27.403. Реализация угрозы возможна, если у нарушителя имеются сведения о системе. Это может быть следствием того, что или в системе используется широко известное общесистемное программное и программно-аппаратное обеспечение, или такие сведения добыты нарушителем в результате их утечки на предыдущих стадиях или на текущей стадии жизненного цикла системы.

Е.2 Оценка допустимого риска нарушения функционирования системы

Е.2.1 Предельно допустимое значение риска нарушения функционирования системы для стадии эксплуатации определяют следующим образом.

Если для системы установлены категории значимости (классы, уровни защищенности), то реализуют принцип дифференцированного задания требований. При этом предельно допустимое значение риска нарушения функционирования системы устанавливают применительно к соответствующей категорией значимости (классу защищенности), которое устанавливают в ТЗ. Для системы с высшей категорией значимости (классом, уровнем защищенности) тем самым предъявляют формальное требование, согласно которому вероятность нарушения функционирования системы при каждой попытке реализации угрозы не должна превышать согласованного заинтересованными сторонами предельно допустимого количественного значения $R_{\Phi 1}^{(\text{тр})}$. Для других категорий значимости (классов, уровней защищенности) по согласованию заинтересованных сторон устанавливают коэффициенты снижения требований γ_k, $k = 2, 3, \ldots K$ таким образом, что для k-й категории значимости (класса, уровня защищенности)

$$R_{\Phi k}^{(\text{тр})} = \gamma_k \cdot R_{\Phi 1}^{(\text{тр})},\ 1 < \gamma_k < \left(1 / R_{\Phi 1}^{(\text{тр})}\right) \text{ для } k = 2, 3, \ldots K,\ R_{\Phi 1}^{(\text{тр})} > 0, \tag{Е.1}$$

где K — количество категорий значимости (классов, уровней защищенности).

Если для этапа эксплуатации определенное в модели угроз прогнозное значение интенсивности попыток реализации u-й угрозы безопасности информации, приводящее к нарушению функционирования системы, составляет величину $\lambda_{\Phi u}$, то предельно допустимое значение вероятности реализации угрозы на стадии эксплуатации системы $P_{\Phi uk}^{(\text{тр})}(T_{\text{экспл}})$ может быть рассчитано по формуле

$$P_{\Phi uk}^{(\text{тр})}(T_{\text{экспл}}) = 1 - \exp\left(-\lambda_{\Phi u} \cdot R_{\Phi k}^{(\text{тр})} \cdot T_{\text{экспл}}\right), \tag{Е.2}$$

где $T_{\text{экспл}}$ — длительность стадии эксплуатации системы.

Для системы, категория значимости (или класс, уровень защищенности) которой не установлена, требования предъявляются в соответствии с низшей категорией значимости.

Е.2.2 Пример Е.1. Пусть в соответствии с постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [9] поставляемая предприятию система отнесена ко второй категории значимости. Продолжительность стадии эксплуатации системы $T_{экспл}$ составляет ориентировочно 10 лет, т. е. около 87600 ч. Необходимо установить предельно допустимую вероятность нарушения функционирования системы, если сведения о системе не относятся к конфиденциальной информации (т. е. общеизвестны).

Для решения задачи примера Е.1 с использованием прецедентного принципа вводят дополнительные предположения. Например, пусть в соответствии с ТЗ $R_{Ф1}^{(тр)} = 10^{-6}$ ***, а интенсивность реализации угроз, приводящих к нарушению функционирования системы,*** $\lambda_{Фu} = 1{,}4 \cdot 10^{-3}$ ***раз в час (1 раз в месяц). По согласованию заинтересованных сторон установлено, что коэффициент снижения требований для второй категории значимости данной системы*** $\gamma_2 = 5$***. Тогда по формуле (Е.1)***

$$R_{Ф2}^{(тр)} = \gamma_2 \cdot R_{Ф1}^{(тр)} = 5 \cdot 10^{-6}.$$

Искомая предельно допустимая вероятность реализации угрозы на стадии эксплуатации (длительностью $T_{экспл}$ ***= 87600 часов) в соответствии с формулой (Е.2) не должна превышать величину:***

$$P_{Фu2}^{(тр)}(T_{экспл}) = 1 - \exp\left(-1{,}4 \cdot 10^{-3} \cdot 5 \cdot 10^{-6} \cdot 87600\right) \approx 0{,}006.$$

Е.2.3 Предельно допустимое значение риска нарушения функционирования системы позволяет определять другие риски, связанные с различными типами нарушения функционирования системы — например, предельно допустимые значения рисков преднамеренного воздействия на системную или пользовательскую информацию, в результате которого система переходит в состояние «Отказ в обслуживании». При этом в модели угроз, формируемой в соответствии с [10], [11], должны быть раздельно определены угрозы, направленные на системную и пользовательскую информацию. Для расчета допустимых значений рисков воздействия на системную и пользовательскую информацию, оцениваемых для стадии эксплуатации системы k-й категории значимости (класса, уровня защищенности) в сравнении с допустимой вероятностью $P_{Фuk}^{(тр.1)}(T_{экспл})$ реализации угроз относительно системной информации и допустимой вероятностью $P_{Фuk}^{(тр.2)}(T_{экспл})$ реализации угроз относительно пользовательской информации используют соотношение

$$P_{Фuk}^{(тр)}(T_{экспл}) = 1 - \left[1 - P_{Фuk}^{(тр.1)}(T_{экспл})\right] \cdot \left[1 - P_{Фuk}^{(тр.2)}(T_{экспл})\right]. \quad (Е.3)$$

Отсюда с учетом формулы (Е.2) для системы k-й категории значимости (класса, уровня защищенности) при практически линейной зависимости малых значений расчетных вероятностей от интенсивностей реализации угроз следует:

$$\lambda_{Фu} R_{Фk}^{(тр)} = \lambda_{Фu}^{(1)} R_{Фk}^{(тр.1)} + \lambda_{Фu}^{(2)} R_{Фk}^{(тр.2)}, \ \lambda_{Фu} = \lambda_{Фu}^{(1)} + \lambda_{Фu}^{(2)}; \quad (Е.4)$$

$$R_{Фk}^{(тр.1)} = R_{Фk}^{(тр)} \cdot \lambda_{Фu}^{(1)} / \lambda_{Фu}; \ R_{Фk}^{(тр.2)} = R_{Фk}^{(тр)} \cdot \lambda_{Фu}^{(2)} / \lambda_{Фu}, \quad (Е.5)$$

где $\lambda_{Фu}$ — суммарная интенсивность попыток реализации угроз, направленных на нарушение функционирования системы;

$R_{Фk}^{(тр)}$ — предельно допустимое значение вероятности нарушения функционирования системы k-й категории значимости при каждой попытке реализации угрозы путем воздействия или на системную, или пользовательскую информацию;

$\lambda_{Фu}^{(1)}$ и $\lambda_{Фu}^{(2)}$ — интенсивности попыток реализации угроз, направленных на нарушение функционирования системы путем воздействия соответственно на системную и пользовательскую информацию;

$R_{Фk}^{(тр.1)}$, $R_{Фk}^{(тр.2)}$ — предельно допустимые вероятности нарушения функционирования системы при каждой попытке реализации угрозы путем воздействия соответственно на системную и на пользовательскую информацию.

Предельно допустимые значения вероятностей воздействия на системную и пользовательскую информации, характеризующие дифференцированные требования к допустимым рискам, определяют по формулам (Е.6) и (Е.7):

$$P_{Фuk}^{(тр.1)}(T_{экспл}) = 1 - \exp\left(-\lambda_{Фu}^{(1)} \cdot R_{Фk}^{(тр.1)} \cdot T_{экспл}\right), \quad (Е.6)$$

$$P_{Фuk}^{(тр.2)}(T_{экспл}) = 1 - \exp\left(-\lambda_{Фu}^{(2)} \ R_{Фk}^{(тр.2)} \cdot T_{экспл}\right). \quad (Е.7)$$

Примечание — За счет умножения интенсивностей попыток реализации угроз $\lambda_{\phi u}^{(1)}$ и $\lambda_{\phi u}^{(2)}$ на вероятности соответственно $R_{\phi k}^{(\text{тр.1})}$ и $R_{\phi k}^{(\text{тр.2})}$ по аналогии с действиями в Д.2.1 происходит «просеивание» изначальных попыток реализации угроз, тем самым в результате произведения осуществляется учет лишь «успешных» попыток реализации угроз. В итоге интенсивности «успешных» попыток уменьшаются по сравнению с их изначальными уровнями $\lambda_{\phi u}^{(1)}$ и $\lambda_{\phi u}^{(2)}$. Именно этот эффект «просеивания» отражен в формулах (Е.4)—(Е.7). Здесь «успешная» реализация угроз по-прежнему рассматривается с точки зрения системного анализа для определения эффективных мер, средств и способов противодействия этой «успешности» — см. примечание в Д.1.3.

Е.2.4 Пример Е.2. Пусть для системы, рассмотренной в примере Е.1, имеющей вторую категорию значимости, определены интенсивности реализации угроз (относительно системной и пользовательской информации), приводящих к нарушению функционирования системы: $\lambda_{\phi u}^{(1)} = 6 \cdot 10^{-4}$ ***раз в час и*** $\lambda_{\phi u}^{(2)} = 8 \cdot 10^{-4}$ ***раз в час соответственно. Кроме того, для пользовательской информации установлено, что предельно допустимое значение вероятности реализации угрозы нарушения функционирования системы в каждой попытке не должно превышать величины*** $R_{\phi 2}^{(\text{тр})} = 5 \cdot 10^{-6}$ ***(см. пример Е.1).***

Требуется определить предельно допустимые вероятности реализации угроз воздействия на системную и пользовательскую информацию.

Для решения задачи примера Е.2 с учетом результатов предыдущего примера Е.1 по формуле (Е.5) имеют место количественные соотношения:

$$\begin{cases} R_{\phi 2}^{(\text{тр.1})} = R_{\phi 2}^{(\text{тр})} \cdot \lambda_{\phi u}^{(1)} / \left(\lambda_{\phi u}^{(1)} + \lambda_{\phi u}^{(2)} \right) = 5 \cdot 10^{-6} \cdot 6 \cdot 10^{-4} / \left(6 \cdot 10^{-4} + 8 \cdot 10^{-4} \right) \approx 2{,}14 \cdot 10^{-6}; \\ R_{\phi 2}^{(\text{тр.2})} = R_{\phi 2}^{(\text{тр})} \cdot \lambda_{\phi u}^{(2)} / \left(\lambda_{\phi u}^{(1)} + \lambda_{\phi u}^{(2)} \right) = 5 \cdot 10^{-6} \cdot 8 \cdot 10^{-4} / \left(6 \cdot 10^{-4} + 8 \cdot 10^{-4} \right) \approx 2{,}86 \cdot 10^{-6}. \end{cases}$$

Предельно допустимые вероятности реализации угроз воздействия на системную и пользовательскую информации рассчитывают по формулам (Е.6)—(Е7) соответственно:

$$P_{\phi uk}^{(\text{тр.1})}(T_{\text{эксп}}) = 1 - \exp\left(-6 \cdot 10^{-4} \cdot 2{,}14 \cdot 10^{-6} \right) \approx 1{,}1 \cdot 10^{-4};$$

$$P_{\phi uk}^{(\text{тр.2})}(T_{\text{эксп}}) = 1 - \exp\left(-8 \cdot 10^{-4} \cdot 2{,}86 \cdot 10^{-6} \cdot 87600 \right) \approx 2{,}1 \cdot 10^{-4}.$$

Эти допустимые значения используют для решения соответствующих задач системного анализа — см. раздел 7.

Е.3 Оценка допустимого риска утечки пользовательской информации

Е.3.1 Предельно допустимое значение риска утечки пользовательской информации, не подлежащей распространению в соответствии с установленными требованиями заинтересованных сторон, определяют с учетом:

- требований заказчика по обеспечению конфиденциальности пользовательской информации на стадии эксплуатации или выведения системы из эксплуатации;
- категории значимости системы, в которой циркулирует конфиденциальная информация, или, если категория значимости не установлена, важности информации для ее обладателей и пользователей.

Примечание — К конфиденциальной информации может относиться информация, содержащая сведения, составляющие тот или иной вид тайны, например, государственной, служебной, коммерческой, профессиональной (банковской или врачебной тайны, тайны связи и др.), а также персональные данные. Вопросы относительно информации, содержащей сведения, составляющие государственную тайну, регулируются специальными документами и в настоящем стандарте не рассматриваются (см. также [9]—[14]).

Е.3.2 Реализация угроз утечки конфиденциальной информации осуществляется или путем непосредственного (физического) несанкционированного доступа к элементам системы (например, к рабочим станциям, серверам, коммуникационным элементам), или путем проведения сетевых атак с других рабочих станций системы или из сети Интернет (для программных систем). Некоторые из способов реализации угроз связаны с нарушением функционирования системы или ее элементов, не обязательно относящихся к подсистеме защиты информации. В связи с этим для определения предельно допустимой вероятности утечки информации сначала определяют допустимые значения вероятностей воздействия на пользовательскую информацию (см. Е.2), которые принимаются за базовые. Полагают, что предельно допустимые значения вероятностей утечки пользовательской информации при каждой попытке реализации угрозы утечки должны быть не выше допустимых значений вероятностей $R_{\phi k}^{(\text{тр.2})}$ реализации угрозы нарушения функционирования системы в каждой попытке (см. Е.2).

Далее в зависимости от категории значимости (класса, уровня защищенности) системы и от того, к какому виду тайны относятся сведения, раскрываемые в результате утечки информации, с участием заказчика предельно допустимые значения вероятностей могут быть скорректированы в сторону их увеличения. Для этого заинтересованные стороны устанавливают коэффициенты важности информации, составляющей тот или иной вид тайны ζ_v, $v = 1, 2, \ldots V$, $\zeta_1 = \zeta_{min} \geq 1$, $\zeta_V = \zeta_{max}$.

После этого для системы с k-й категорией значимости (с k-м классом, уровнем защищенности) предельно допустимое значение $R^{(тр.2)}_{конф\,kv}$ вероятности утечки пользовательской информации, содержащей сведения, составляющие v-й вид тайны, при каждой попытке реализации угрозы определяют из соотношения:

$$R^{(тр.2)}_{конф\,kv} = \zeta_v \cdot R^{(тр.2)}_{фk}, \text{ где } 1 < \zeta_v \leq 1/R^{(тр.2)}_{фk}, \ v = 1, 2, \ldots V. \quad (Е.8)$$

Предельно допустимое значение вероятности реализации угрозы утечки конфиденциальной информации, содержащей сведения, составляющие v-й вид тайны, за время эксплуатации системы $T_{эксплл}$ при интенсивности $\lambda_{конф\,kv}$, попыток реализации определяют из соотношения:

$$P^{(тр.2)}_{конф\,kv}(T_{эксплл}) = 1 - \exp\left(-\lambda_{конф\,kv} \cdot R^{(тр.2)}_{конф.kv} \cdot T_{эксплл} / \zeta_v\right). \quad (Е.9)$$

Тем самым вычисляемые по формулам (Е.8), (Е.9) значения определяют формальные требования к допустимому риску утечки пользовательской информации.

Е.3.3 Пример Е.3. В автоматизированной системе коммерческого предприятия к конфиденциальной отнесена информация, содержащая сведения, составляющие коммерческую тайну, и персональные данные. Система отнесена к третьей категории значимости. Необходимо определить предельно допустимые значения показателей риска нарушения утечки указанной информации, циркулирующей в функционирующей системе, если интенсивность попыток копирования пользовательской информации, составляющей коммерческую тайну, равна $\lambda_{конф\,31} = 8 \cdot 10^{-4}$ раз в час, а интенсивность попыток копирования персональных данных равна $\lambda_{конф\,32} = 10^{-3}$ раз в час.

Для решения задачи примера Е.3 с использованием прецедентного принципа вводят дополнительные предположения. Пусть предельно допустимое значение риска воздействия на пользовательскую информацию при каждой попытке реализации угрозы задано и составляет величину $R^{(тр.2)}_{ф3} = 2{,}1 \cdot 10^{-4}$ (см. пример Е.2). Заказчик установил коэффициент важности для информации, составляющей коммерческую тайну, равным $\zeta_1 = 5$, т. е. предельно допустимое значение вероятности утечки этой информации в соответствии с формулой (Е.8) должно составлять не более $R^{(тр.2)}_{конф\,31} = \frac{2{,}1 \cdot 10^{-4}}{5} = 4{,}2 \cdot 10^{-5}$. Для информации, составляющей персональные данные, заказчиком установлен коэффициент, равным $\zeta_2 = 3$, при этом предельно допустимое значение вероятности утечки персональных данных при каждой попытке реализации угрозы в соответствии с формулой (Е.8) не должно превышать $R^{(тр.2)}_{конф\,32} = \frac{2{,}1 \cdot 10^{-4}}{3} = 7 \cdot 10^{-5}$.

Искомое предельно допустимое значение риска реализации угрозы утечки сведений, составляющих коммерческую тайну, за время эксплуатации системы $T_{эксплл} = 87600$ ч в соответствии с формулой (Е.9) составит величину

$$P^{(тр.2)}_{конф\,31}(T_{эксплл}) = 1 - \exp\left(-8 \cdot 10^{-4} \cdot 87600 \cdot 4{,}2 \cdot 10^{-5}\right) \approx 2{,}9 \cdot 10^{-5},$$

а для персональных данных предельно допустимое значение риска составит

$$P^{(тр.2)}_{конф\,32}(T_{эксплл}) = 1 - \exp\left(-10^{-3} \cdot 87600 \cdot 7 \cdot 10^{-5}\right) \approx 6{,}1 \cdot 10^{-3}.$$

Эти допустимые значения используют для решения соответствующих задач системного анализа — см. раздел 7.

Е.4 Оценка допустимого риска нарушения надежности реализации процесса определения системных требований в части защиты информации

Е.4.1 При оценке и формировании требований к предельно допустимому значению риска нарушения надежности реализации процесса определения системных требований в части ЗИ делают предположение, что надежность реализации процесса будет нарушена, если при эксплуатации будет нарушено функционирование системы (из-за реализации угроз безопасности информации) и/или на какой-либо стадии жизненного цикла произойдет утечка пользовательской информации, циркулирующей в системе и не подлежащей распространению в соответствии с установленными требованиями заинтересованных сторон системы.

Е.4.2 Предельно допустимое значение риска нарушения надежности реализации процесса определения системных требований в части ЗИ $P_{инт}^{(тр)}$ с учетом соотношения (Д.17) определяют по формуле

$$P_{инт}^{(тр)} = 1 - \left[1 - P_{пр}^{(тр)}(T_{экспл})\right] \cdot \left[1 - P_{конф}^{(тр)}(T_{вых})\right], \quad (Е.10)$$

где $P_{пр}^{(тр)}(T_{экспл})$ — предельно допустимое значение условной вероятности нарушения надежности реализации процесса определения системных требований в части ЗИ применительно к стадии эксплуатации продолжительностью $T_{экспл}$ с учетом возможности утечки информации о системе или внедрения на предыдущих стадиях вредоносной программы, используемой для реализации угроз на стадии эксплуатации.

С учетом соотношения (Д.1):

$$P_{пр}^{(тр)}(T_{экспл}) = 1 - \prod_{u=1}^{U_{экспл}^{(ф)}} \left[1 - P_{фu}^{(тр)}\left(\frac{T_{экспл}}{T_s}\right)\right] \cdot \prod_{u=1}^{U_{экспл}^{(конф)}} \left[1 - P_{конф\,u}^{(тр)}\left(\frac{T_{экспл}}{T_s}\right)\right]; \quad (Е.11)$$

$P_{конф}^{(тр)}(T_{вых})$ — предельно допустимое значение вероятности реализации угрозы утечки информации о системе на стадии выведения ее из эксплуатации (s = 6) продолжительностью $T_{вых}$.

С учетом соотношения (Д.18):

$$P_{конф}^{(тр)}(T_{вых}) = 1 - \exp\left(-\lambda_{вых} \cdot R_{вых}^{(тр)} \cdot T_{вых}\right), \quad (Е.12)$$

где $\lambda_{вых}$ — ожидаемая интенсивность попыток реализации угроз утечки информации на стадии выведения системы из эксплуатации (подлежит определению для осуществления моделирования);

$R_{вых}^{(тр)}$ — предельно допустимое значение вероятности утечки информации в каждой попытке реализации угрозы на стадии выведения системы из эксплуатации.

Предельно допустимые значения условных вероятностей того, что на стадии эксплуатации (т. е. за период $T_{экспл}$) будет реализована хотя бы одна угроза, направленная на нарушение функционирования системы $P_{фu}^{(тр)}(T_{экспл} / T_s) \equiv P_{фu}^{(тр)}(T_{экспл})$ или хищение конфиденциальной информации $P_{конф\,u}^{(тр)}(T_{экспл} / T_s) \equiv P_{конф\,u}^{(тр)}(T_{экспл})$, при условии, что на этой же стадии добывается информация, используемая для реализации указанных угроз, определяется из соотношений (Д.7)—(Д.12):

$$P_{фu}^{(тр)}(T_{экспл}) = 1 - \lambda_{фu} \cdot R_{фu}^{(тр)} \cdot \left[\lambda_{фu} \cdot R_{фu}^{(тр)} - \lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)}\right]^{-1} \cdot \exp\left[-\lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)} \cdot T_{экспл}\right] +$$
$$+ \lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)} \cdot \left[\lambda_{фu} \cdot R_{фu}^{(тр)} - \lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)}\right]^{-1} \cdot \exp\left[-\lambda_{фu} \cdot R_{фu}^{(тр)} \cdot T_{экспл}\right], \quad (Е.13)$$

если $\lambda_{фu} \cdot R_{фu}^{(тр)} \neq \lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)}$;

$$P_{фu}^{(тр)}(T_{экспл}) = 1 - \left[1 + \lambda_{фu} \cdot R_{фu}^{(тр)} \cdot T_{экспл}\right] \cdot \exp\left(-\lambda_{фu} \cdot R_{фu}^{(тр)} \cdot T_{экспл}\right), \quad (Е.14)$$

если $\lambda_{фu} \cdot R_{фu}^{(тр)} = \lambda_{ф\,доб} \cdot R_{ф\,доб}^{(тр)}$;

$$P_{конф\,u}^{(тр)}(T_{экспл}) = 1 - \left[\lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} - \lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)}\right]^{-1} \cdot \lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} \times$$
$$\times \exp\left(-\lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)} \cdot T_{экспл}\right) + \left[\lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} - \lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)}\right]^{-1} \times$$
$$\times \lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)} \cdot \exp\left(-\lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} \cdot T_{экспл}\right), \quad (Е.15)$$

если $\lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} \neq \lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)}$;

$$P_{конф\,u}^{(тр)}(T_{экспл}) = 1 - \left[1 + \lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} \cdot T_{экспл}\right] \cdot \exp\left(-\lambda_{конф\,u} \cdot R_{конф\,u}^{(тр)} \cdot T_{экспл}\right), \quad (Е.16)$$

если $\lambda_{конф\,u} \cdot R_{конф\,доб}^{(тр)} = \lambda_{конф\,доб} \cdot R_{конф\,доб}^{(тр)}$.

где $R^{(тр)}_{ф\,u}$ и $R^{(тр)}_{конф\,u}$ — предельно допустимые значения вероятностей реализации угроз для стадии эксплуатации системы в каждой из попыток такой реализации, направленных соответственно на нарушение функционирования системы и утечку конфиденциальной информации;

$\lambda_{фu}$ и $\lambda_{конф\,u}$ — ожидаемые для стадии эксплуатации системы интенсивности попыток реализации угроз, направленных соответственно на нарушение функционирования системы и утечку конфиденциальной информации;

$R^{(тр)}_{ф\ доб}$ и $R^{(тр)}_{конф\ доб}$ — предельно допустимые значения вероятностей того, что в каждой попытке угроза выявления информации о системе, необходимой для последующей реализации угроз соответственно нарушения ее функционирования или хищения конфиденциальной информации, будет реализована на стадии эксплуатации системы;

$\lambda_{ф\ доб}$ и $\lambda_{конф\ доб}$ — ожидаемые интенсивности попыток реализации угроз на стадии эксплуатации системы, направленных на добывание информации, используемой соответственно для нарушения функционирования системы и выявления конфиденциальной информации.

Предельно допустимые значения вероятностей того, что на стадии эксплуатации будет реализована хотя бы одна угроза, направленная на нарушение функционирования системы $P^{(тр)}_{фu}(T_{эксп\,л} / T_s)$ или хищения конфиденциальной информации $P^{(тр)}_{конф\,u}(T_{эксп\,л} / T_s)$, при условии, что информация, используемая для реализации указанных угроз, добывается на предыдущих стадиях, определяют по аналогии с соотношениями (Д.4) и (Д.6):

$$P^{(тр)}_{фu}(T_{эксп\,л} / T_s) = P^{(тр)}_{фu}(T_{эксп\,л}) \cdot \left\{1 - \prod_{s<l} \prod_{j(u)}^{J_{фu}(s)} \left[1 - P^{(тр.s)}_{фj(u)}(T_s)\right]\right\}; \quad (Е.17)$$

$$P^{(тр)}_{конф\,u}(T_{эксп\,л} / T_s) = P^{(тр)}_{конф\,u}(T_{эксп\,л}) \cdot \left\{1 - \prod_{s<l} \prod_{j(u)}^{J_{конф\,u}(s)} \left[1 - P^{(тр.s)}_{конф\,j(u)}(T_s)\right]\right\}, \quad (Е.18)$$

где $P^{(тр)}_{фu}(T_{эксп\,л})$ — предельно допустимое значение вероятности того, что угроза нарушения функционирования системы на стадии эксплуатации будет реализована при наличии информации, необходимой и используемой для этой реализации.

С учетом соотношения (Д.18)

$$P^{(тр)}_{фu}(T_{эксп\,л}) = 1 - \exp\left[-\lambda_{фu} \cdot R^{(тр)}_{фu} \cdot T_{эксп\,л}\right], \quad (Е.19)$$

$P^{(тр.s)}_{фj(u)}(T_s)$ — предельно допустимое значение вероятности реализации $j(u)$-й угрозы утечки на s-й стадии жизненного цикла (предшествующей стадии эксплуатации) информации, используемой для реализации u-й угрозы нарушения функционирования системы на стадии эксплуатации, $j(u) = 1, 2, \ldots J_{фu}(s)$. Рассчитывается по формуле

$$P^{(тр.s)}_{фj(u)}(T_s) = 1 - \exp\left[-\lambda^{(s)}_{фj(u)} \cdot R^{(доп.s)}_{фj(u)} \cdot T_s\right], \quad (Е.20)$$

где $\lambda^{(s)}_{фj(u)}$ — интенсивность реализации $j(u)$-й угрозы утечки на s-й стадии жизненного цикла (предшествующей стадии эксплуатации с номером i) информации, используемой для реализации u-й угрозы нарушения функционирования системы на стадии эксплуатации;

$R^{(доп.s)}_{фj(u)}$ — предельно допустимое значение вероятности утечки информации на s-й стадии в каждой попытке реализации угрозы в интересах добывания сведений, используемых для реализации u-й угрозы нарушения функционирования системы на стадии эксплуатации;

$P^{(тр)}_{конф\,u}(T_{эксп\,л})$ — предельно допустимое значение вероятности того, что угроза утечки информации на стадии эксплуатации системы будет реализована при наличии информации, необходимой и используемой этой реализации. Рассчитывается по формуле

$$P^{(тр)}_{конф\,u}(T_{эксп\,л}) = 1 - \exp\left[-\lambda_{конф\,u} \cdot R^{(тр)}_{конф\,j(u)} \cdot T_{эксп\,л}\right]; \quad (Е.21)$$

$P^{(тр.s)}_{конф.j(u)}(T_s)$ — предельно допустимое значение вероятности реализации $j(u)$-й угрозы утечки на s-й стадии жизненного цикла (предшествующей стадии эксплуатации, обозначенной номером i) информации, используемой для реализации u-й угрозы утечки конфиденциальной информации на стадии эксплуатации, $j(u) = 1, 2, \ldots J_{конф\,u}(s)$. Рассчитывается по формуле

$$P^{(\text{тр}.s)}_{\text{конф}\,j(u)}(T_s) = 1 - \exp\left[-\lambda^{(s)}_{\text{конф}\,j(u)} \cdot R^{(\text{тр}.s)}_{\text{конф}\,j(u)} \cdot T_s\right], \quad \text{(Е.22)}$$

где $\lambda^{(s)}_{\text{конф}\,j(u)}$ — интенсивность реализации $j(u)$-й угрозы утечки на s-й стадии жизненного цикла (предшествующей стадии эксплуатации с номером i) информации о системе, используемой для реализации u-й угрозы хищения конфиденциальной информации на стадии эксплуатации;

$R^{(\text{тр}.s)}_{\text{конф}\,j(u)}$ — предельно допустимое значение вероятности утечки информации о системе на s-й стадии при каждой попытке реализации угрозы в интересах добывания сведений, используемых для реализации u-й угрозы хищения конфиденциальной информации на стадии эксплуатации.

Е.4.3 Пример Е.4. Пусть для системы, рассмотренной в примере Е.1 и имеющей вторую категорию значимости, предельно допустимая вероятность реализации угрозы на стадии эксплуатации рассчитана и равна $P^{(\text{тр})}_{\text{ср}}(T_{\text{эксопл}}) = 0{,}006$ ***, см. результаты примера Е.1. Предельно допустимая вероятность реализации угрозы утечки информации о системе на стадии вывода ее из эксплуатации определяется интенсивностью*** $\boldsymbol{\lambda_{\text{вых}}}$ ***возникновения угроз, равной трем случаям в месяц (т. е.*** $\boldsymbol{\lambda_{\text{вых}} = 4{,}2 \cdot 10^{-3}}$ ***раза в час). Заинтересованными сторонами установлена предельно допустимая вероятность реализации такой угрозы в каждой попытке на уровне*** $R^{(\text{тр})}_{\text{вых}} = 3 \cdot 10^{-3}$ ***. Продолжительность периода вывода из эксплуатации*** $\boldsymbol{T_{\text{вых}}}$ ***составляет 3 месяца (приблизительно 2160 часов). Необходимо рассчитать предельно допустимую вероятность нарушения реализации процесса определения системных требований к системе для периода вывода системы из эксплуатации с учетом возможной реализации угроз безопасности информации на стадии ее эксплуатации.***

Для решения задачи примера Е.4 возможно использование формулы (Е.9) с соответствующей заменой задаваемого периода прогноза:

$$P^{(\text{тр})}_{\text{инт}}(T_{\text{вых.}}) = 1 - (1 - 0{,}006) \cdot \left[1 - \exp\left(-4{,}2 \cdot 10^{-3}\ \ 3 \cdot 10^{-3} \cdot 2160\right)\right] = 0{,}029.$$

В итоге проведенного в примере системного анализа предельно допустимый риск нарушения надежности реализации процесса определения системных требований обоснован на уровне 0,03 за период вывода из эксплуатации, равный трем месяцам.

Расчетные допустимые значения рисков, связанных с защитой информации, в полной мере могут быть использованы в качестве исходных данных для моделирования различных системных процессов и решения задач системной инженерии — см. примеры для разных областей приложения в ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59347, ГОСТ Р 59349.

Приложение Ж
(справочное)

Методические указания по прогнозированию рисков и определению перечня существенных угроз безопасности информации

Ж.1 Риск реализации угроз нарушения безопасности информации в системе, рассматриваемый в процессе определения системных требований, оценивают вероятностью реализации угроз в сопоставлении с возможным ущербом за задаваемый период прогноза. В связи с тем, что на практике в ходе обоснования системных требований необходимые исходные данные для оценки размеров возможного ущерба от реализации угроз могут отсутствовать, следует использовать любые возможные подходы. Например, один из возможных подходов сводится к тому, что при расчете рисков учитывают только определенные неприемлемые ущербы. В этом случае оценка риска сводится к расчету только вероятности реализации соответствующих угроз с использованием комплекса аналитических или имитационных моделей (см. Д.3). Другой подход основан на экспертных процедурах оценки возможных ущербов в сочетании с балльными методами оценки реализации угроз безопасности информации в системе (см. Д.4).

Ж.2 Оценка рисков реализации угроз безопасности информации с использованием комплекса аналитических моделей сводится к расчету вероятностей реализации в условиях отсутствия мер защиты информации и прогнозируемого применения выбираемых мер защиты в зависимости от специфики системы и особенностей ее функционирования (см. 5.6, 6.3, 7.5, Д.3). Определенными возможностями для моделирования угроз безопасности информации обладает аппарат сетей Петри—Маркова, отражающих использование составных марковских и полумарковских процессов. Использование этого аппарата целесообразно в том случае, когда имеют место логические условия выполнения моделируемого процесса (см. Д.3).

Ж.3 Для парирования угроз безопасности информации в системе применяют разнообразные меры ЗИ, которые разделяют на:

- организационные, реализуемые без применения программных и программно-аппаратных средств защиты и без проведения соответствующих настроек программно-аппаратной среды системы;
- организационно-технические, реализуемые путем проведения организационных мероприятий, проведением реконфигурации системы, изменением соответствующих настроек операционной системы, а также с применением программных и программно-аппаратных средств защиты;
- технические, реализуемые только проведением реконфигурации системы, изменением соответствующих настроек операционной системы и путем применения программных и программно-аппаратных средств защиты.

Возможный вариант классификации типовых мер защиты от угроз безопасности информации приведен на рисунке Ж.1.

Если мера ЗИ реализуется с применением технических средств, то при обосновании системных требований следует ориентироваться на сертифицированные средства защиты, состав которых указан в Государственном реестре средств ЗИ. Некоторые типовые средства ЗИ с классификацией приведены на рисунке Ж.2.

Ж.4 Результаты оценки рисков реализации угроз в условиях отсутствия мер ЗИ, планируемых при обосновании системных требований, используют при определении перечня существенных угроз безопасности информации на каждой стадии и в течение всего жизненного цикла системы. Порядок определения перечня существенных угроз приведен на рисунке Ж.3 и состоит в следующем:

- сначала определяют перечень потенциальных угроз безопасности информации. Для этого могут быть использованы сведения из национального Банка данных угроз или описания угроз, которые встречались в аналогичных системах и описаны в различных источниках, в т. ч. в сети Интернет;
- далее проводят анализ стадий жизненного цикла системы и выявляют источники, которые могут иметь место для каждой потенциальной угрозы на каждой стадии, а также наличие уязвимостей в процессе разработки, производства, поставки системы и ее эксплуатации. Если источники угроз и указанные уязвимости (которые могут быть использованы для реализации угроз безопасности информации) имеют место, то угрозы относят к потенциальным и формируется перечень потенциальных угроз;
- оценивают возможный ущерб от реализации угрозы (например, с использованием экспертных методов — см. Д.4). Если такой ущерб неприемлем для разработчика или заказчика системы, то угрозу относят к потенциально опасной. Составляют перечень потенциально опасных угроз;
- для перечня потенциально опасных угроз разрабатывают одну или несколько математических моделей их реализации, оценивают риски реализации угроз — см. приложение Д;
- определяют предельно допустимые риски реализации угроз на каждой стадии и в течение всего жизненного цикла системы, с которым сравнивают оцениваемые риски (для каждой угрозы и/или задаваемого перечня угроз в возможных сценариях нарушения безопасности информации).

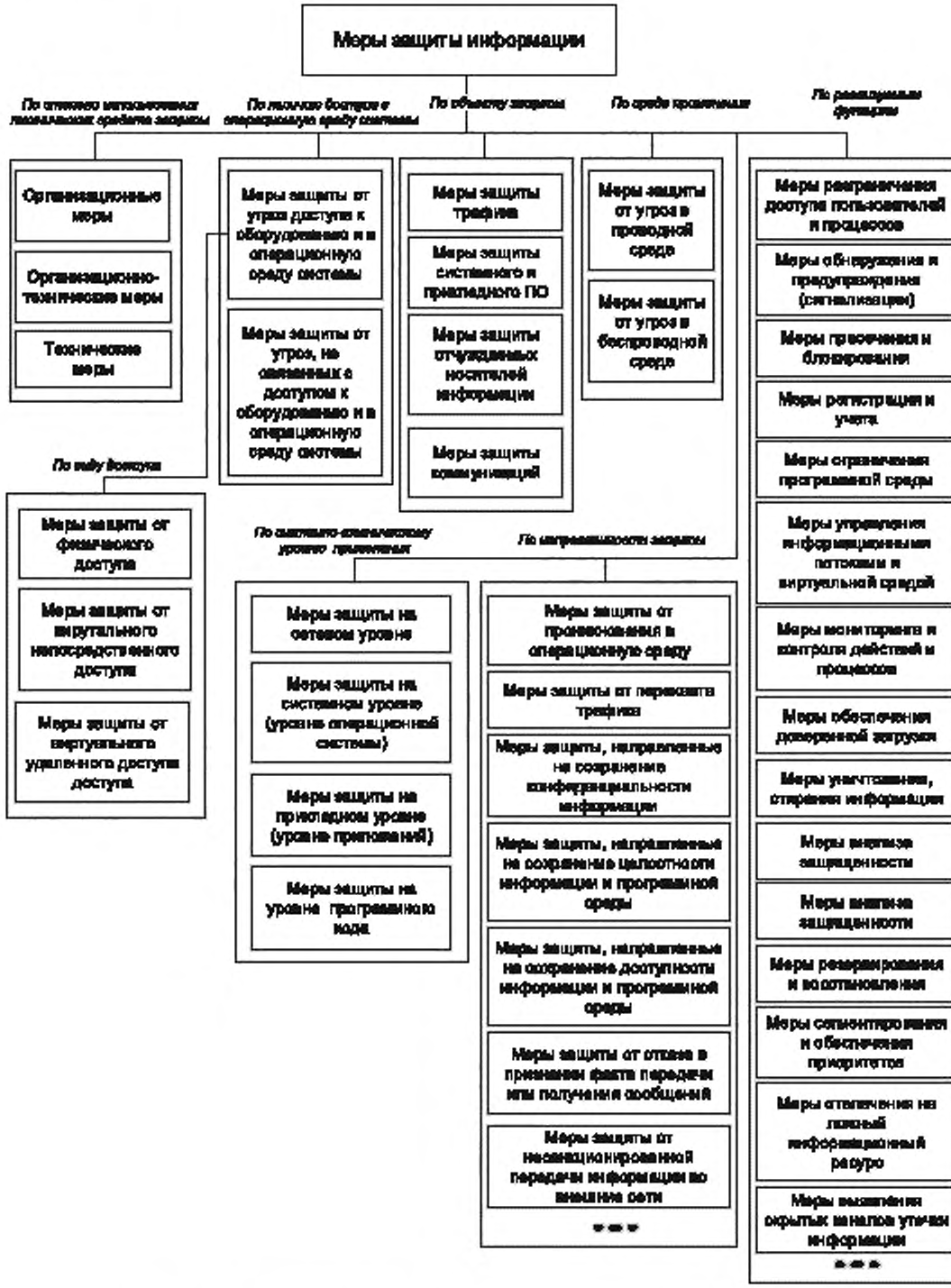


Рисунок Ж.1 — Примерная классификация типовых мер защиты информации в системе

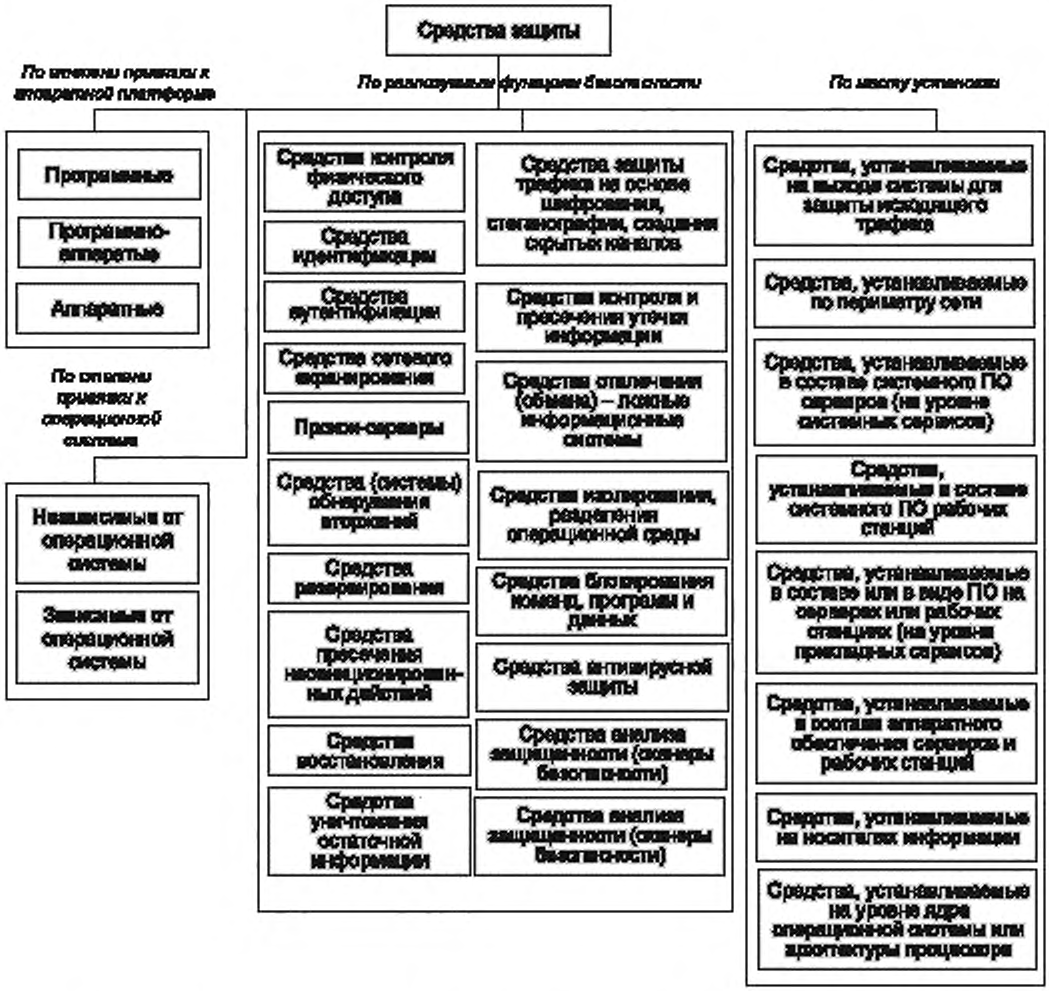


Рисунок Ж.2 — Типовые средства защиты информации, которые могут применяться в системе

Если вероятности реализации угроз выше предельно допустимых значений, то такие угрозы признают существенными. Составляют перечень существенных угроз и формируют модели угроз для системы — см. приложение Е.

Примечание — Другие модели, методы и примеры прогнозирования рисков и способы решения различных задач системного анализа приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59347, ГОСТ Р 59356.

С учетом специфики системы допускается использование любых научно обоснованных методов, моделей, методик, отвечающих целям системного анализа.

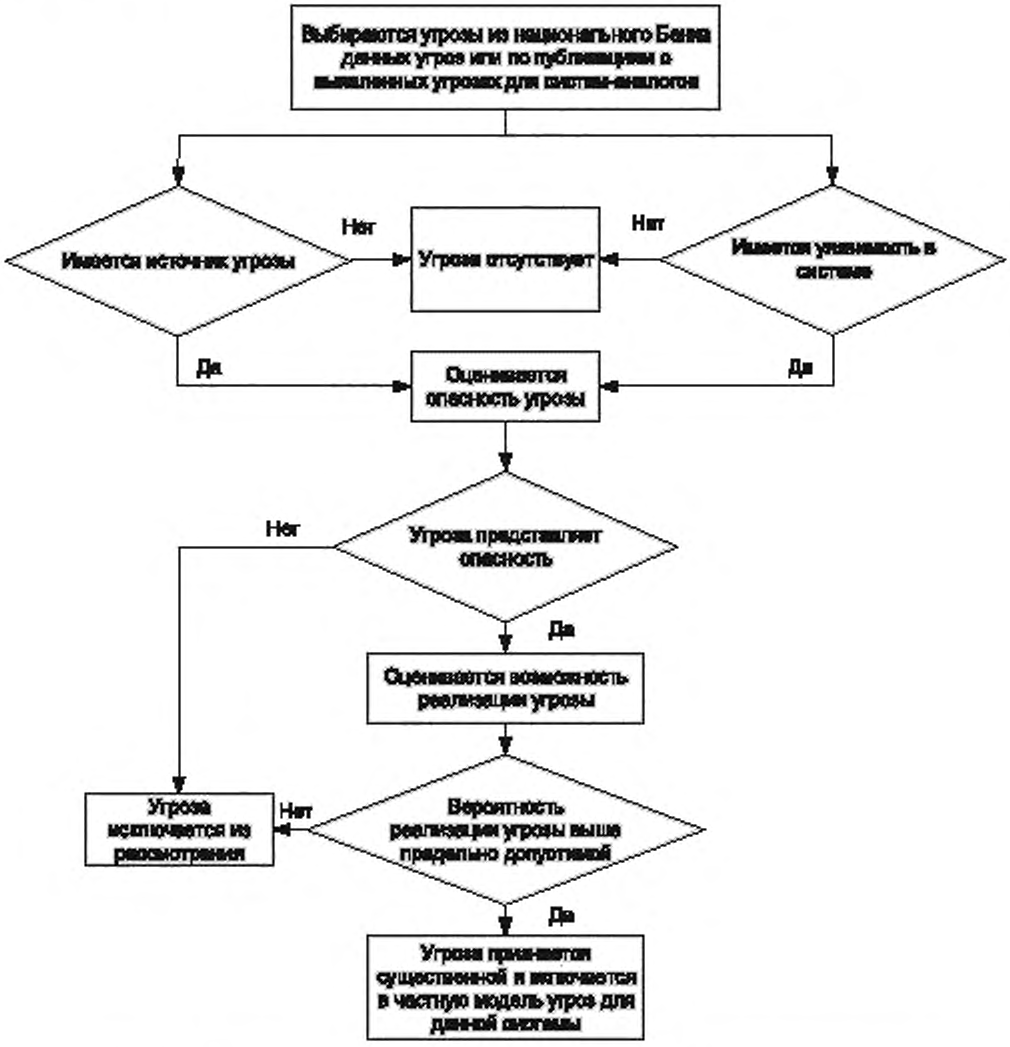


Рисунок Ж.3 — Порядок определения перечня существенных угроз безопасности информации

Библиография

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

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

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

[4] Федеральный закон от 26 июля 2017 г. № 152-ФЗ «О персональных данных»

[5] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований по защите персональных данных при их обработке в информационных системах персональных данных»

[6] Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

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

[8] Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

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

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

[11] 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)

[12] 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)

[13] 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

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

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

Ключевые слова: актив, безопасность, защита информации, модель, процесс определения системных требований, риск, система, системная инженерия, требования, управление, угрозы безопасности информации

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

Сдано в набор 11.05.2021. Подписано в печать 27.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 6,73.

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.
www.gostinfo.ru info@gostinfo.ru