ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 11231— 2024

Менеджмент риска

МЕТОД ВЕРОЯТНОСТНОЙ ОЦЕНКИ РИСКА НА ПРИМЕРЕ КОСМИЧЕСКИХ СИСТЕМ

[ISO 11231:2019, Space systems — Probabilistic risk assessment (PRA), IDT]

Издание официальное

Москва
Российский институт стандартизации
2024

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 августа 2024 г. № 1089-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 11231:2019 «Космические системы. Вероятностная оценка риска (PRA)» [ISO 11231:2019 «Space systems — Probabilistic risk assessment (PRA), IDT].

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВЗАМЕН ГОСТ Р ИСО 11231—2013

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

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.rst.gov.ru)

Содержание

Введение

В структурированных процессах менеджмента риска обычно используют качественные и количественные методы оценки риска в ходе выбора оптимальных решений для обеспечения безопасности и вероятности успешного целевого применения космической системы (см. ИСО 17666). Наиболее систематизированным и комплексным из этих методов является метод вероятностной оценки риска (PRA).

PRA за последние три десятилетия стала основным аналитическим методом для идентификации и анализа риска в проектах и сложных системах. Успешный опыт применения данного метода в менеджменте риска был подтвержден во многих отраслях промышленности, включая космическую, энергетическую, нефтехимическую, а также сферу обеспечения безопасности. Метод PRA используется для идентификации и оценивания риска путем выявления его основных составляющих, чтобы эффективно распределять ресурсы для устранения существенных составляющих риска и не расходовать их на незначительные. Кроме того, метод PRA может стать основой для количественной оценки неопределенности событий и их последовательности, которые важны для безопасности системы. Позволяя количественно оценить неопределенность, метод PRA дает принимающим решения лицам информацию об источниках неопределенности и о значимости инвестиционных ресурсов для снижения неопределенности. Таким образом, метод PRA дополняет традиционный анализ безопасности и может быть использован для принятия решений в области безопасности. Применение метода PRA для анализа безопасности позволяет определить оценку вероятности и значимости событий, а также их последствий, которые могут оказать неблагоприятные воздействия на безопасность.

Метод PRA отличается от анализа надежности в двух важных аспектах:

a) метод PRA позволяет более точно оценить неопределенность как для отдельных событий, так и для системы в целом;

b) в методе PRA применены более информативные оценки, которые количественно определяют показатели, связанные с возникновением неблагоприятных последствий (например, гибель людей, невыполнение основной задачи проекта), в отличие от узко определенных показателей эффективности функционирования системы (например, средней наработки до отказа).

Метод PRA отличается от метода анализа опасностей, в соответствии с которым идентифицируют и оценивают значимые показатели редких событий, исследуя их так, будто они произошли без учета вероятности их реализации. Кроме того, при проведении анализа опасностей нельзя гарантировать полноту набора сценариев инцидентов. Результаты PRA являются иными и могут быть непосредственно применены при распределении ресурсов и принятии других решений менеджмента риска, основанных на более широком спектре данных о показателях.

С помощью метода PRA возможно идентифицировать слабые и уязвимые места системы, которые могут неблагоприятно воздействовать на безопасность, функционирование и выполнение поставленных целей. Полученные результаты помогают разработать эффективные стратегии менеджмента риска, направленные на снижение риска и позволяющие ответственному персоналу принимать обоснованные решения по оптимальному использованию ресурсов.

Метод PRA может быть успешно применен при оценке риска сложных систем, к которым возможно применить сценарии реализации опасных событий с низкой вероятностью возникновения и значимыми последствиями, или при оценке комплексных сценариев, состоящих из цепочки событий, которая может неблагоприятно воздействовать на безопасность системы больше, чем каждое событие по отдельности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

МЕТОД ВЕРОЯТНОСТНОЙ ОЦЕНКИ РИСКА НА ПРИМЕРЕ КОСМИЧЕСКИХ СИСТЕМ

Risk management. Probabilistic risk assessment method on example of space systems

Дата введения — 2025—03—01

1 Область применения[1)]

Настоящий стандарт обеспечивает выполнение требований к процессу менеджмента риска, установленных в ИСО 17666, и дополняет их в ситуациях, когда необходимо применение количественной оценки риска.

В настоящем стандарте определены принципы, процесс, способы выполнения и требования к количественной оценке риска, а также приведено детальное описание метода PRA применительно к обеспечению безопасности. Метод PRA может применяться для менеджмента риска проекта, связанного со стоимостью и плановыми сроками, однако пояснение деталей такого использования не входит в область применения настоящего стандарта.

В настоящем стандарте установлены основные требования и процедуры использования метода PRA для оценки безопасности или риска невыполнения проекта в области космических систем. Настоящий стандарт применим ко всем международным космическим проектам, предусматривающим:

- разработку космических транспортных средств для перемещения людей в космическом пространстве;
- разработку космических и внеземных планетарных обитаемых станций;
- разработку космических средств выведения на орбиту, использующих для работы или транспортирующих ядерные материалы;
- другие виды разработок в соответствии с требованиями руководства или потребителей[2)].

При выполнении указанных работ необходимо учитывать сценарии, последовательности событий или действия, которые могут привести к травмированию или гибели людей (космонавтов, пилотов, населения и персонала), потере критического или ценного оборудования и имущества. При выполнении других видов работ PRA выполняют по усмотрению руководителей проекта.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

ISO 17666, Space systems — Risk management (Космические системы. Менеджмент риска)

---

1) *При применении настоящего стандарта следует учитывать, что порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти установлен постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».*

2) *Информация по результатам выполнения работ в соответствии с пунктом 6.3 и разделом 8 может иметь ограниченное использование, т. к. раскрывает конфиденциальную информацию о космическом комплексе.*

Издание официальное

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины и определения по ИСО 17666, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для использования в целях стандартизации по следующим адресам:

- платформа онлайн-просмотра ИСО доступна по адресу: https://www.iso.org/obp;
- Электропедия МЭК доступна по адресу: https://www.electropedia.org/.

3.1.1 **приемлемый риск** (acceptable risk): Риск безопасности, значимость и *вероятность* (3.1.3) которого могут быть на разумной основе приняты при отсутствии долгосрочных и необратимых негативных последствий для здоровья людей, окружающей среды и планеты Земля в настоящее время и в будущем.

[ИСО 14620-2:2011, 3.1, изменено — удален пример]

3.1.2 **экспертная оценка** (expert judgment): Данные о вероятности, полученные систематизированным и структурированным способами на основании суждений и оценок специалистов.

Примечание 1 — Под структурированным способом получения данных понимают использование определенного методического подхода; под систематизированным способом получения данных понимают регулярное получение данных.

Примечание 2 — Математическое объединение экспертных оценок предпочтительнее, чем объединение на основе свойств и характеристик или согласованного решения.

3.1.3 **вероятность** (probability): Мера, характеризующая возможность наступления события, условия или сценария, которые в случае возникновения влекут за собой позитивные или негативные последствия.

3.1.4 **пороговое значение вероятности** (probability reference frame): Значение вероятности, относительно которого определяют *вероятность* (3.1.3).

Примечание 1 — Пороговое значение вероятности связано со структурой анализа вероятности. Типичным пороговым значением, используемым в космических проектах, является «вероятность выполнения основной задачи проекта».

3.1.5 **риск** (risk): Нежелательная ситуация или обстоятельства, которые имеют как вероятность возникновения, так и потенциально негативные последствия для проекта.

Примечание 1 — Риски возникают вследствие неопределенности из-за отсутствия предсказуемости или контроля событий. Риски присущи любому проекту и могут возникнуть в любое время в течение жизненного цикла проекта; снижение неопределенности снижает риск.

[ИСО 17666:2016, 3.1.12]

3.1.6 **вклад в риск** (risk contribution): Мера снижения *вероятности* (3.1.3) основного последствия, если событие, определяющее соответствующую составляющую риска, не произойдет.

Примечание 1 — Вклад в риск показывает величину возможного снижения риска при отсутствии рассматриваемой составляющей риска и прямо пропорционален ей. Основными составляющими риска являются риски событий, имеющих большой вклад в риск, отсутствие которых приводит к существенному снижению риска.

Примечание 2 — Систематическая оценка вкладов в риск позволяет ранжировать по риску конструкции и функциональные элементы системы. Это дает возможность идентифицировать высокий риск и/или уязвимые места системы, которые затем могут быть использованы как направления повышения безопасности.

3.1.7 **составляющая риска** (risk contributor): Риск единичного события или набора событий, от которых зависит исследуемый риск.

Примечание — Составляющие риска могут быть упорядочены в соответствии с их *вкладом в риск* (3.1.6).

3.1.8 **менеджмент риска** (risk management): Систематическая и итеративная оптимизация ресурсов проекта, выполняемая в соответствии с установленной политикой в области менеджмента риска проекта.

[ИСО 17666:2016, 3.1.5]

3.1.9 **сценарий риска** (risk scenario): Последовательность или комбинация событий, ведущих от первоначальной причины к нежелательному последствию.

Примечание — Причиной может быть одно событие или что-то, что приводит в действие неактивную проблему.

[ИСО 17666:2016, 3.1.13]

3.1.10 **риск [нарушение] безопасности** (safety risk): Мера потенциальных последствий опасности с учетом *вероятности* (3.1.3) связанного с ней несчастного случая, вреда, причиненного людям, и ущерба, нанесенного общественной и частной собственности и окружающей среде.

Пример — Ожидаемое количество потерь.

Примечание 1 — Риск (нарушение) безопасности всегда связан с определенным сценарием или набором сценариев реализации опасности. Риск, соответствующий единственному сценарию, называют «риском отдельного сценария». Риск, соответствующий набору рисков отдельных сценариев и их последствий, называют «совокупным риском».

Примечание 2 — Величину риска (нарушения) безопасности характеризуют значимостью и *вероятностью* (3.1.3) последствий.

[ИСО 14620-2:2011, 3.30, изменено — удалены примечания 1 и 2; добавлены новые примечания 1 и 2; добавлен пример]

3.1.11 **заинтересованная сторона** (interested party; stakeholder): Лицо или организация, которые могут получить преимущества или потери при реализации опасного события и связанных с ним последствий.

Пример — Потребители, владельцы, работники в организации, поставщики, банки, регулирующие органы, союзы, партнеры или сообщество, которое может включать конкурентов или группы противодействия.

[ИСО 9000:2015, 3.2.3, изменено — удалено примечание 1]

3.1.12 **неопределенность** (uncertainty): Недостаток информации, вызванный неточностью входных параметров и/или анализа процесса.

Примечание 1 — Неопределенность может быть представлена в виде интервала с верхней и нижней границами значений или в виде распределения неопределенности.

3.1.13 **составляющая неопределенности** (uncertainty contributor): Неопределенность риска единичного события или набора единичных событий, от которой зависит неопределенность риска основного последствия.

Примечание 1 — Составляющие неопределенности могут быть ранжированы друг относительно друга в соответствии с их *вкладом в неопределенность* (3.1.14).

3.1.14 **вклад в неопределенность** (uncertainty contribution): мера снижения неопределенности вероятности основного последствия в предположении, что неопределенность вероятности исследуемого события равна нулю.

Примечание 1 — Вклад в неопределенность указывает на возможное снижение общей неопределенности или составляющих неопределенности и прямо пропорционален им. Важные составляющие неопределенности соответствуют событиям, имеющим высокий вклад в неопределенность и допускающим существенное снижение неопределенности.

Примечание 2 — Систематическая оценка вклада в неопределенность позволяет ранжировать по неопределенности данные и источники информации.

3.2 Сокращения

АВПКО — анализ видов, последствий и критичности отказов (FMECA — failure mode, effects, and criticality analysis);

IE — входное событие (initiating event);

MLD — главная диаграмма (master logic diagrams);

PRA — вероятностная оценка риска (probabilistic risk assessment);

P(A) — вероятность события A (probability of event A);

P(A/B) — вероятность события A при условии реализации события B (conditional probability of event A given event B has occurred);

RM — менеджмент риска (risk management).

4 Принципы вероятностной оценки риска

4.1 Общие положения

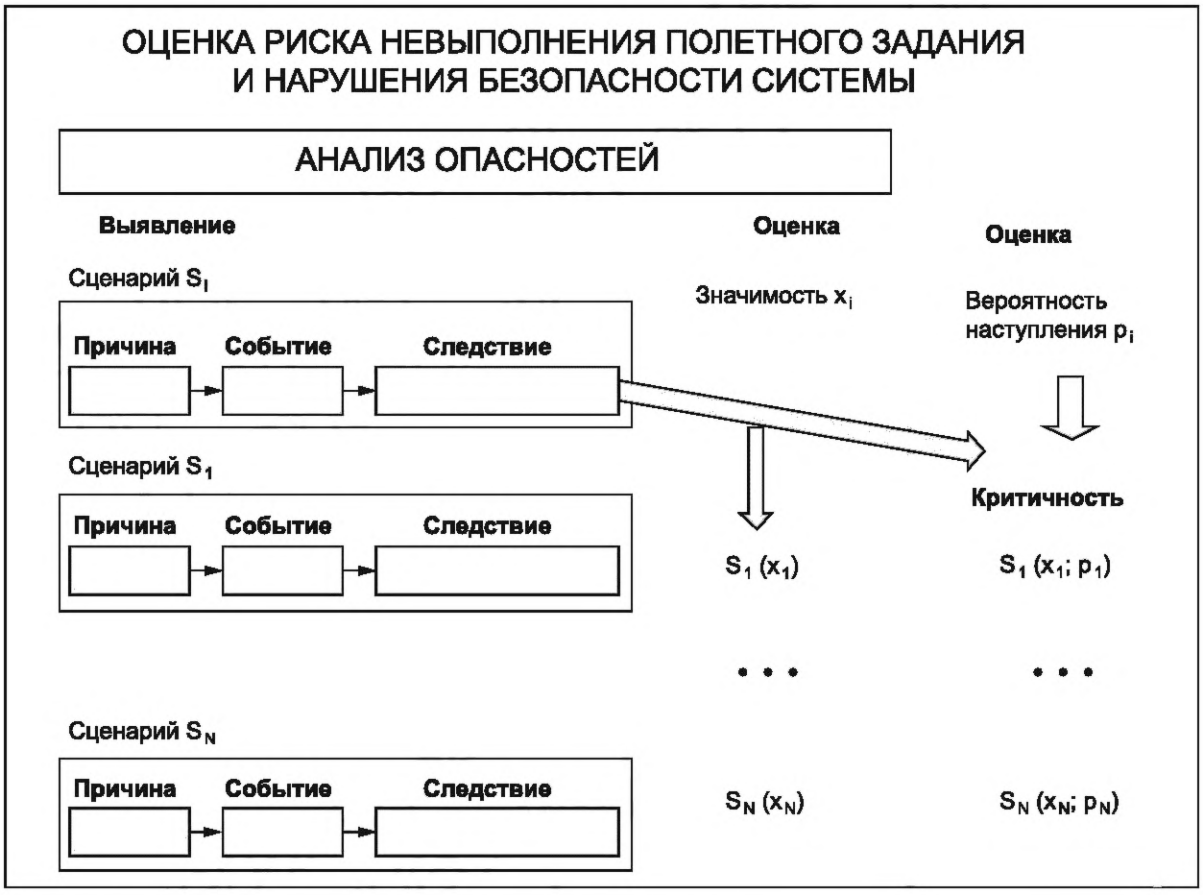
Метод вероятностной оценки риска помогает руководителям и техническим специалистам использовать результаты оценки риска в своей работе и при принятии решений на всех стадиях жизненного цикла [исследование и обоснование разработки, разработка, производство, эксплуатация изделий, применение (хранение) материалов, капитальный ремонт (для изделий, подлежащих капитальному ремонту)], в процессе менеджмента, при оценке затрат и планировании работ (см. ИСО 17666).

В настоящем стандарте методология PRA предназначена для оценки технических рисков, связанных с успешным целевым применением космической системы и ее безопасностью.

4.2 Концепция оценки риска для успешного целевого применения и безопасности космической системы

В настоящем разделе рассматривается применение PRA для успешного целевого применения космической системы и рисков (нарушения) безопасности системы. Оценку успешности целевого применения космической системы и рисков (нарушения) безопасности системы дополняют детерминированный анализ видов и последствий отказов (FMEA) и анализ опасности (HA), добавляя вероятностную оценку к детерминированной оценке в виде анализа видов, последствий и критичности отказов АВПКО в случае первого и оценку риска опасности в случае второго. Эта вероятностная оценка обеспечивает принятие решений с учетом риска.

Взаимосвязь между детерминированными и вероятностными методами оценивания видов отказов/опасностей показана на рисунке 1.



S_i — сценарий i; S_1 — сценарий 1; S_N — сценарий N со значимостью последствий = x_i и вероятностью = p_i; $S_1(x_1)$ — значимость последствий сценария 1; $S_1(x_1;p_1)$ — риск сценария 1; $S_N(x_N)$ — значимость последствий сценария N; $S_N(x_N;p_N)$ — риск сценария N

Рисунок 1 — Взаимосвязь между детерминированными и вероятностными методами оценивания типов отказов/степени опасности

Оценка риска (нарушения) безопасности может быть использована как для оценки риска индивидуальных сценариев реализации опасностей, так и для оценки совокупного риска набора сценариев реализации опасностей.

Оценка риска индивидуальных сценариев может быть выполнена с помощью схем ранжирования значимости последствий и вероятности реализации сценариев при использовании сети или матрицы риска и индексов риска, описанных в ИСО 23460 и ИСО 14620-1. Однако матрицы и индексы риска не могут быть использованы для объединения индивидуальных составляющих риска сценария или объединения различных сценариев для оценки совокупного риска. Эти методы не допускают использования результатов промежуточных вычислений.

Оценка совокупного риска, соответствующего определенному набору сценариев, требует применения подхода PRA. Этот подход обеспечивает основу для выявления и ранжирования составляющих риска. Важные составляющие риска впоследствии могут быть использованы для совершенствования конструкции и функционирования системы с точки зрения ее безопасности. Рассчитанный совокупный риск может быть соотнесен с вероятностными показателями безопасности или критериями приемлемости. На этапе 1 процесса менеджмента риска высшее руководство или потребители определяют приемлемость риска. Риск может быть использован в качестве исходных данных для количественного определения показателей безопасности в моделях принятия решений.

Представление оценки совокупного риска невыполнения проекта или нарушения безопасности системы показано на рисунке 2. В соответствии с рисунком при оценке риска (нарушения) безопасности используют сценарии реализации опасности для моделирования отдельных последовательностей событий, необходимых и достаточных для возникновения установленных нежелательных последствий. Сценарий может быть представлен как «логическое пересечение» начальной причины или исходного события и необходимых условий промежуточных событий, приводящих к соответствующему последствию. Таким образом, совокупный риск является логическим объединением рисков индивидуальных сценариев, приводящих к одному и тому же последствию.

Вероятностная оценка риска для сложных систем обычно помогает идентифицировать сценарии с применением деревьев событий или диаграммы последовательности событий и деревьев неисправностей для получения логических моделей формирования определенных нежелательных последствий нарушения безопасности. В соответствии с представленным выше описанием для количественного определения вероятности конечного состояния системы вероятность исходного события (т. е. причины) умножают на вероятность каждого последующего промежуточного события при условии реализации последовательности предыдущих событий по каждому сценарию. Для каждого сценария значимость последствий обычно определяют на основе характеристик происходящих физических процессов (явлений) и особенностей сценария. Совокупные последствия определяют путем суммирования последствий всей совокупности сценариев, используя данные аналогичных событий.

Для оценки вероятности событий обычно используют различные источники данных. Типичными источниками данных являются данные предыдущих испытаний системы [т. е. данные измерений или прямых наблюдений в процессе испытаний, экспериментов, исследований (см. ИСО 16192)], данные о других системах или проектах (данные о системах-аналогах, данные моделирования физических процессов) и экспертные оценки (т. е. оценки вероятности специалистами в конкретной области). События рассматривают в соответствии со сценарием реализации опасности, т. е. вероятность события оценивают как вероятность при условии реализации последовательности предыдущих событий.

При определении оценки совокупного риска проводят систематическую идентификацию и оценку неопределенности, которую выполняют двумя способами. При определении оценки вероятности событий сценария определяют оценку соответствующих неопределенностей в виде интервалов или распределений вероятностей. Полученную неопределенность используют для определения оценки вероятности последствий.

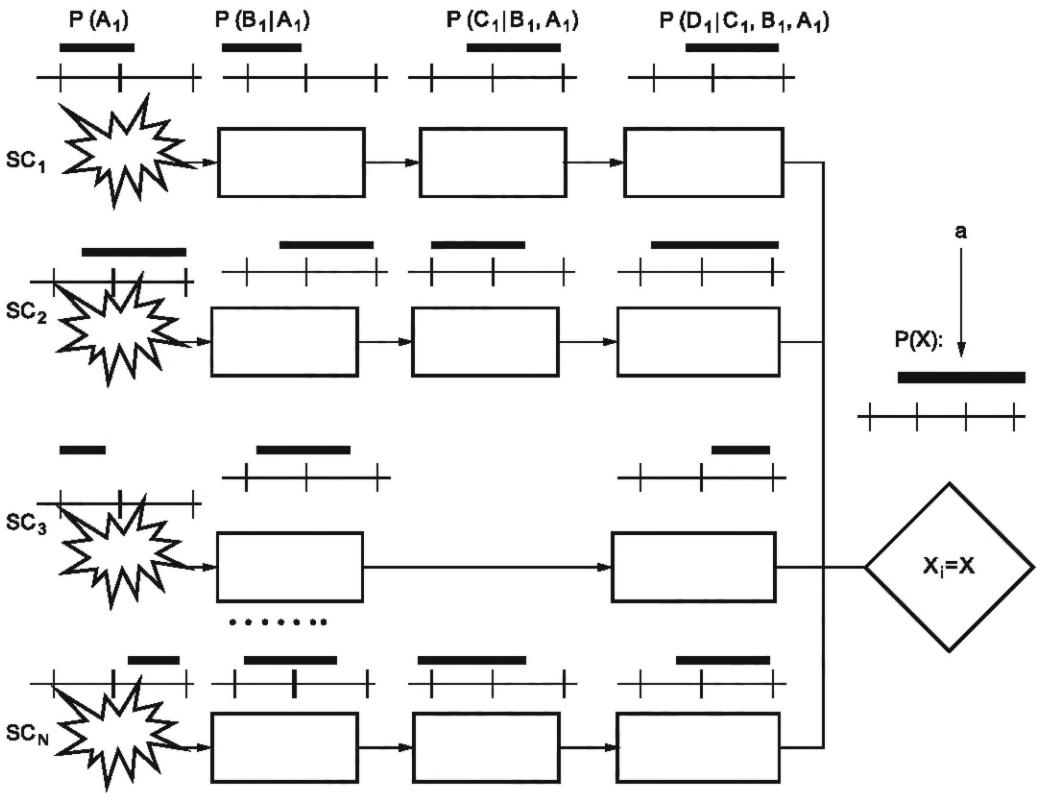
Количественную оценку совокупного риска проводят на основе расчета вероятностей и последствий. В результате вычислений могут быть получены точечные оценки или распределения вероятностей (неопределенности). Распределение неопределенности может быть описано с помощью параметров, например среднего или квантиля установленного уровня в правой части распределения. Значение квантиля в правой части распределения неопределенности, соответствующей совокупному риску для установленного уровня доверия, используют для выполнения гарантированного подхода при принятии решений о приемлемости риска. Гарантированный подход предполагает, что для значений риска следует рассматривать наихудшие варианты, чтобы гарантировать, что система соответствует согласованным целям в области риска или выбор критериев приемлемости риска и вариантов проекта

выполнен правильно. Более высокая неопределенность значения совокупного риска формирует соответствующее значение параметров распределения, которое будет использовано для принятия риска или его сопоставления с другими рисками или критериями.

Относительная значимость события или сценария для совокупного риска определяется их вкладом в неопределенность совокупного риска. Вклады в совокупный риск характеризуют возможность повышения безопасности системы, т. е. возможность снижения совокупного риска при устранении риска данного события или сценария. Аналогично параметры конструкции и функционирования системы могут быть ранжированы с точки зрения снижения риска на основе анализа составляющих событий и их вклада в совокупный риск.

Влияние неопределенности риска конкретного события или сценария на неопределенность совокупного риска определяется их вкладом в неопределенность совокупного риска. По вкладу в неопределенность идентифицируют и ранжируют события, представляющие собой основные источники неопределенности вероятности последствий, которые могут быть устранены или для которых неопределенность, соответствующая их риску, может быть существенно уменьшена. Снижение неопределенности последствий напрямую связано с использованием менее жестких значений параметров или квантилей распределения неопределенности.

Составляющие риска и неопределенности идентифицируют на основе их ранжирования. Важными составляющими риска и неопределенности являются те события или соответствующие им компоненты системы, которым соответствуют наибольший риск и наибольшие возможности снижения неопределенности совокупного риска.



SC_1 — сценарий 1; SC_2 — сценарий 2; SC_3 — сценарий 3; SC_N — сценарий N; P(X) — полная вероятность, логическая сумма вероятностей всех сценариев от 1 до N; $P(A_1)$ — вероятность события A_1, исходное событие; $P(B_1 | A_1)$ — вероятность события B_1 при условии реализации события A_1; $P(C_1 | B_1, A_1)$ — вероятность события C_1 при условии реализации событий B_1 и A_1; $P(D_1 | C_1, B_1, A_1)$ — вероятность события D_1 при условии реализации событий C_1, B_1 и A_1

[a] Репрезентативное точечное значение.

Рисунок 2 — Пример оценки совокупного риска

4.3 Общий процесс вероятностной оценки риска

Как показано на рисунке 3, выполнение метода PRA начинают с определения множества IE, которые могут вызвать изменения в состоянии системы, т. е. в ее функциональном состоянии или конфигурации. Затем для каждого IE анализ продолжают определением последующих событий (отказов), которые могут привести к нежелательным последствиям. После этого определяют величины значимости последствий этих сценариев, а также частоты (вероятности) их возникновения. Частоты и последствия интегрируют в представление профиля риска системы. Профиль риска оценивают на предмет неопределенности и затем используют для принятия решений в менеджменте риска.

Рисунок 3 — Этапы общего процесса вероятностной оценки риска

5 Цели, способы применения и преимущества вероятностной оценки риска

5.1 Цели вероятностной оценки риска

Целями PRA являются:

- идентификация и оценка риска (нарушения) (безопасности или невыполнения проекта), который представляет собой риск реализации отдельных идентифицированных сценариев или совокупный риск реализации набора сценариев;
- идентификация составляющих риска и их неопределенности, а также соответствующих областей риска при проектировании и эксплуатации системы;
- ранжирование составляющих риска и их неопределенности в порядке убывания их значимости;
- идентификация и определение приоритетности для мероприятий по снижению риска.

5.2 Применение результатов вероятностной оценки риска

Результаты вероятностной оценки риска используют:

- для оценки уровня безопасности или риска невыполнения основной задачи проекта в количественном (вероятностном) выражении;
- снижения уровня риска невыполнения задачи проекта и нарушения безопасности или успешного целевого применения космической системы за счет снижения риска;

- определения и внедрения проектных и функциональных требований, спецификаций, концепций, процедур и т. д.;
- обеспечения количественных данных при определении требований к обеспечению безопасности и выполнении задачи проекта посредством:
  определения применимости требований к обеспечению безопасности и выполнению задачи проекта,
  выполнения требований к обеспечению безопасности и выполнению задачи проекта;
- верификации результатов PRA и демонстрации соответствия требованиям;
- поддержки при принятии решений, связанных с безопасностью и целевым применением космической системы;
- поддержки документов и отчетов по вопросам безопасности посредством документированных доказательств;
- поддержки сертификации безопасности системы путем обеспечения документированных доказательств;
- поддержки информирования и отслеживания рисков;
- обеспечения входных данных при разработке общего менеджмента риска проекта.

5.3 Преимущества вероятностной оценки риска

Преимущества PRA заключаются в следующем:
- обеспечение количественных данных для оценки рисков и их приемлемости;
- более эффективное распределение обязанностей по обеспечению безопасности;
- эффективное распределение расходов на обеспечение безопасности пропорционально снижению риска;
- эффективное и последовательное внедрение мер безопасности в систему;
- обеспечение наглядного представления количественных показателей сценариев опасных событий;
- количественная идентификация уязвимых мест в системе и ее компонентах;
- оценка безопасности системы и ее подсистем на этапе их разработки;
- количественное сравнение эффективности действий по снижению риска.

6 Требования и подробный процесс вероятностной оценки риска

6.1 Требования к вероятностной оценке риска

В настоящем стандарте установлены следующие требования к PRA:
a) PRA должна проводиться в соответствии с требованиями пункта 6.3;
b) PRA должна быть задокументированна в соответствии с требованиями раздела 8.

6.2 Краткий обзор процесса вероятностной оценки риска

Основные задачи PRA описаны в 6.3. Эти задачи используют для выполнения этапов 1—4 общей схемы последовательности операций процесса PRA, как описано в 4.3 и показано на рисунке 3. Планирование PRA должно приводить к ряду мероприятий, которые соизмеримы с системной удельной стоимостью/критичностью для выполнения задачи проекта и содержанием технических данных/степенью завершенности жизненного цикла. Такое планирование иногда называют адаптацией процесса на основе возможностей (см. ISO/TS 18667). Пример определений степеней удельной стоимости/критичности для выполнения задачи проекта в области космических систем приведен в приложении А (взят из ISO/TS 18667). Руководство по адаптации процесса PRA на основе возможностей приведено в приложении В (взято из ISO/TS 18667).

6.3 Основные задачи вероятностной оценки риска

6.3.1 Общие положения

Подробная схема последовательности задач процесса PRA показана на рисунке 4. Краткое описание каждой из девяти основных задач этого процесса представлено в 6.3.2—6.3.10.

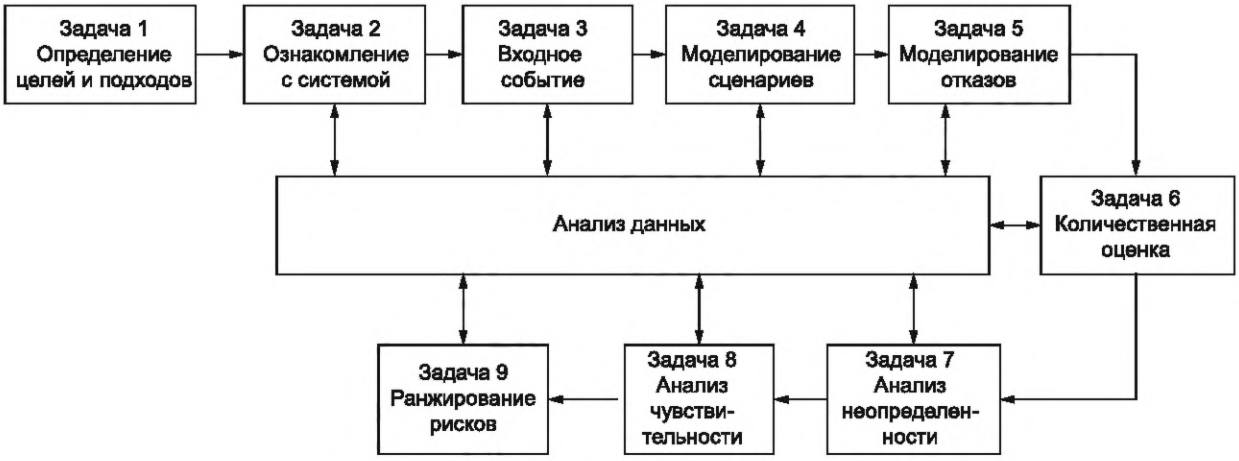


Рисунок 4 — Основные задачи этапов процесса вероятностной оценки риска

6.3.2 Задача 1 — определение целей и подходов

Первоначальной задачей при использовании PRA является определение целей, области применения и подхода к анализу, т. е. планирование PRA. Цели оценки риска обеспечивают четкое понимание цели и предполагаемого применения результатов. Область применения определяет профиль задачи проекта и систему(ы) или ее (их) части, которые будут включены в анализ. Эти два элемента обеспечивают основу для определения и выбора показателей исследуемых последствий. Эти показатели последствий могут включать в себя данные о причинении вреда людям (например, травмы, болезни или смерть), об ухудшении возможностей выполнения задачи проекта, невыполнении задачи проекта, материальном ущербе или других неблагоприятных последствиях.

В зависимости от целей и области применения PRA, а также используемых конфигураций системы и ограничений во времени следует определить руководящие принципы для рассмотрения входных событий (например, определить необходимость включения в анализ внешних событий, таких как микрометеоритный дождь). Результаты задачи 1 должны быть проанализированы соответствующими руководителями проекта и ответственными за обеспечение безопасности системы и выполнение основной задачи проекта до начала проведения оценки.

Задача 1 включает:

a) идентификацию целей вероятностной оценки риска путем определения предполагаемой цели и использования результатов анализа;

b) идентификацию области применения и степени детализации анализа путем определения границ и режимов безопасного функционирования системы (исследуемую часть конструкции и области функционирования системы) и уровня детализации сценариев опасных событий и связанного с ними анализа;

c) идентификацию показателя(ей) последствий для анализа, включая типы последствий и необходимость оценки рисков для отдельных сценариев развития опасности и/или совокупных рисков специфических неблагоприятных последствий (например, невыполнение основной задачи проекта, потеря средства доставки, гибель экипажа), в том числе:

1) идентификацию используемых систем координат, параметров или матрицы рисков (на основе значимости последствий и вероятности реализации сценария),
2) идентификацию установленных целевых показателей совокупного риска или критериев приемлемости риска (на основе вероятностных целевых показателей и критерия для конкретного последствия);

d) идентификацию связанных источников информации и данных;

e) документирование одобренного плана PRA.

6.3.3 Задача 2 — изучение системы

Изучение системы является следующим этапом. Изучение включает в себя анализ и всю информацию о конструктивных параметрах и функционировании системы, включая техническую и технологическую документацию, а также правила эксплуатации и планы действий в чрезвычайных ситуациях. Если метод PRA применяют для системы, которая находится в эксплуатации, техническая информация должна быть основана на информации о разработке и эксплуатации системы. Если метод PRA исполь-

зуют на этапе проектирования, то техническая информация, необходимая для оценки, должна быть основана на технической документации с учетом предполагаемого функционирования системы. Рекомендуется провести проверку и по возможности визуальный контроль анализируемой системы. Целью этих действий является всестороннее изучение задачи проекта и используемых систем, а также понимание состояний и критериев достижения успеха, необходимых для надлежащего завершения задачи проекта в целом. На стадии изучения системы идентифицируют особенности функционирования системы, их взаимозависимость, роль персонала в процессе функционирования (командование и управление, техническое обслуживание) и любые изменения конфигурации системы, которые могут произойти на различных стадиях, этапах или режимах задачи проекта. Критерии успешного выполнения задачи проекта и функционального состояния системы служат основой для разработки функциональных и системных моделей.

Задача 2 включает:

a) идентификацию и описание области применения анализа, конфигурации и эксплуатации систем (функциональная и физическая структура в соответствии с графиком выполнения задачи проекта), включая стадии выполнения задачи проекта и рабочие конфигурации, составные части и функции системы, физические зоны и т. д.;

b) определение критериев успешного выполнения основной задачи проекта наряду с вкладом и критериями успешности каждой системы, необходимой для завершения основной задачи проекта.

6.3.4 Задача 3 — выявление входного события

Следующим этапом является идентификация и анализ набора входных событий, которые могут привести к реализации сценариев опасных событий. Эти события инициируют последовательность дальнейших опасных событий, приводящих к определенным конечным состояниям (показателям последствий). Существует несколько способов выявления входных событий. Если PRA проводится на существующей системе, которая эксплуатируется в течение некоторого времени, то анализ прошлого опыта, происшествий и истории эксплуатации может помочь выявить входные события. Если анализ проводится для новых проектов, возможно использование прошлого опыта эксплуатации аналогичных систем в аналогичных условиях или с аналогичными областями применения. Наряду с опытными данными для выявления входных событий рекомендуется использовать систематические методы, например MLD и АВПКО. В методе MLD события отображают в виде иерархического нисходящего дерева, показывающего общие типы нежелательных событий в верхней части, переходящего ко все более подробному описанию событий на нижних уровнях и отображающего предполагаемые входные события в нижней части. С помощью метода АВПКО проводят системный анализ отказов компонентов и оценивают их влияние на функционирование системы.

При выявлении нескольких входных событий, ведущих к сценариям с одинаковым конечным состоянием, можно исключить события с очень низкой вероятностью. Независимые входные события могут быть сгруппированы в соответствии со сходством сложностей, которые они представляют для системы, т. е. входных событий, которые приводят к одинаковой реакции системы. В случае, если входные события рассматриваются как группа, их частоты допускается суммировать для получения частоты группы входных событий.

Задача 3 включает:

a) выявление и оценку входных событий, которые могут запустить последующие сценарии опасных событий, с использованием опытных данных и систематических методов (использование соответствующих исходных данных из существующего анализа опасности, подготовленного в соответствии с методами MLD и АВПКО);

b) оценку вероятности наступления выявленных входных событий и исключение событий с очень низкой относительной вероятностью (или частотой);

c) объединение входных событий с одинаковым воздействием на систему в группы и определение вероятностей (частот) наступления событий в группах.

6.3.5 Задача 4 — моделирование сценариев

Моделирование сценариев опасных событий представляет собой индуктивный процесс, в котором обычно используют метод анализа дерева событий. Построение дерева событий начинают с входного события, и далее события проходят через сценарий, последовательность успешных выполнений задач или отказов, промежуточных событий (также называемых поворотными или главными событиями), пока не будут достигнуты конечные состояния. Деревья событий обычно учитывают временну́ю последовательность поворотных или главных событий, которые представляют функциональное или системное поведение всей системы. Иногда для описания сценария опасного события используют графический

инструмент, называемый диаграммой последовательности событий (ESD — event sequence diagram), поскольку диаграмма такого типа лучше поддается техническому осмыслению, чем дерево событий. Диаграмма ESD логически эквивалентна дереву событий и должна быть преобразована в дерево событий для количественной оценки. Другим типом инструментов индуктивного моделирования, который также используют, является структурная схема надежности.

Задача 4 включает:

a) моделирование для каждого входного события (или объединенной группы событий) примерной временной последовательности и соответствующего состояния (успешное выполнение задачи или отказ) ключевых событий (т. е. действий персонала, структуры, систем, компонентов), необходимых для предотвращения потенциальных последствий входного события;

b) оценку условной физической (механистической) реакции системы на физическое воздействие входных событий, измененной выявленными средствами предупредительного контроля (т. е. действиями персонала, структурами, системами, компонентами), и определение величины и характеристик последующей физической реакции (т. е. возможности взрыва, возгорания, потери контроля, потери кислорода и т. д.) для тех опасных последовательностей, которые предположительно могут привести к неблагоприятным потенциальным последствиям;

c) моделирование условной реакции (успешное выполнение задачи или отказ) средств управления (т. е. действий персонала, структур, систем, компонентов), имеющихся или разработанных для снижения неблагоприятных потенциальных последствий, которые могут быть вызваны реакцией физической системы, для тех реакций физической системы, которые могут привести к потенциальным последствиям.

6.3.6 Задача 5 — моделирование отказов

Моделирование причин отказов и неисправностей (или их дополнений, успехов) каждого ключевого события или вершины дерева событий является дедуктивным процессом. Существует несколько инструментов дедуктивного моделирования, которые могут быть использованы для оценки отказов вершины событий, таких как Марковские цепи, структурные схемы надежности и деревья неисправностей. Анализ дерева отказов является наиболее распространенным методом. Дерево отказов состоит из трех частей. Верхняя часть представляет собой основное событие, которое соответствует отказу ключевого события (или вершины дерева событий) в сценарии опасного события. Средняя часть состоит из промежуточных событий (неисправностей), которые в совокупности вызывают отказ события, расположенного непосредственно над ним. Эти события связаны через логические вентили (например, вентили AND и OR) с событиями, расположенными выше, и с событиями в нижней части дерева отказов, называемыми базовыми событиями. Могут существовать несколько уровней промежуточных событий для описания отказа основного (вершины) события. Возникновение базовых событий в конечном итоге приведет к возникновению верхних событий в соответствии с логикой дерева отказов. Затем деревья отказов связывают со сценариями опасных событий и упрощают (с использованием булевых методов) для поддержки количественной оценки.

Задача 5 включает:

a) выявление и регистрацию сопутствующего входного события и предшествующих событий в сценарии опасного события для каждого ключевого события или вершины дерева событий. Эти события обеспечивают начальные и граничные условия, необходимые для оценки их неудач (или их дополнений, успехов). Кроме того, необходима регистрация критериев успешного функционирования (определенных в задаче 2) для функционирования основных или главных событий, которые также необходимы для оценивания;

b) разработку модели отказа (т. е. дерева отказов) для каждого ключевого события или вершины дерева событий, логической комбинации промежуточных неисправностей, которые могут вызвать верхнее событие. В зависимости от моделируемой функции или системы может существовать несколько уровней промежуточных событий;

c) выявление базовых событий (отказов или неисправностей) наряду с их критериями успеха для начальных и граничных условий, связанных с основным событием;

d) связывание моделей дерева отказов для поворотных событий или событий вершины дерева событий с соответствующей частью модели дерева событий.

6.3.7 Задача 6 — количественная оценка

Количественная оценка относится к процессу оценки частоты возникновения и величины значимости последствий нежелательных конечных состояний для сценариев опасных событий. Частота возникновения каждого конечного состояния рассчитывается с использованием подхода, основанного на

построении дерева отказов, в результате чего получается логическое произведение частоты входного события и (условных) вероятностей каждого ключевого события на пути последовательности событий от входного события до конечного состояния. Модели отказов [дерево (деревья) отказов] для поворотных событий обеспечивают логические комбинации базовых событий, необходимые для количественной оценки поворотных событий (через процесс связывания). Величины значимости нежелательных конечных состояний (последствий) для последовательностей опасных событий обычно оцениваются посредством детерминированных расчетов с учетом физической реакции оцениваемой системы и функционирования систем, определенных или разработанных для смягчения последствий. Все последовательности с одинаковыми конечными состояниями затем группируются, т. е. их вероятности логически суммируются в вероятность репрезентативного конечного состояния.

Задача 6 включает:

a) выполнение оценки булевыми методами связанной последовательности событий [дерева (деревьев) событий] и моделей отказов [дерева (деревьев) отказов] для каждого входного события. В результате этой оценки будут получены множества базовых событий (называемые минимальными множествами вырезок событий), приводящих к нежелательным конечным состояниям. Эти минимальные множества представляют опасные последовательности в базовых событиях;

b) оценку частоты возникновения каждого минимального множества вырезок событий путем логического объединения частоты входного события и вероятности отказа для связанных с ним базовых событий. Типичные источники данных для вероятности отказа включают предыдущий опыт работы с конкретной системой (т. е. измеренные или непосредственно наблюдаемые данные соответствующих испытаний или опыта и извлеченные уроки), данные из других систем или проектов (т. е. экстраполяция из общих баз данных, данных о подобии или физических моделей) и экспертную оценку (т. е. прямую оценку вероятности специалистами в данной области);

c) оценку типа и величины значимости последствий;

d) группировку последовательностей с одинаковым конечным состоянием и логическое суммирование их вероятностей для оценки общей вероятности наступления каждого репрезентативного конечного состояния.

6.3.8 Задача 7 — анализ неопределенности

Одной из целей PRA является разработка реалистичных моделей, учитывающих неопределенность событий. Поэтому вероятностная модель риска фактически является моделью анализа неопределенности. Признание того, что анализ неопределенности является основной составляющей вероятностной модели риска и его оценки, закладывает основу для надлежащего применения результатов PRA в процессе принятия решений RM. Аналитик PRA должен найти способы количественной оценки и представления неопределенностей, связанных с аналитическими исходными данными, моделями и степенью знаний, таким образом, чтобы результаты анализа риска были понятны и пригодны для использования лицами, принимающими решения. Все результаты PRA, представленные лицам, принимающим решения, должны включать оценку общей степени неопределенности и давать представление о том, какие источники неопределенности имеют решающее значение для результатов. Для проведения анализа неопределенности обычно применяют методы моделирования Монте-Карло.

Задача 7 включает:

a) учет неопределенности данных при оценке частоты встречаемости каждого минимального набора вырезок событий. При этом необходимо разработать соответствующие распределения или представления неопределенности для базовых событий во множествах минимальных вырезок событий;

b) логическое объединение распределения неопределенности для входного события с распределениями неопределенности для вероятностей отказов, связанных с базовыми событиями. Существует несколько методов для выполнения этих расчетов, включая аналитические методы и моделирование Монте-Карло;

c) определение неопределенностей в величине значимости нежелательных конечных состояний (последствий);

d) оценку вклада неопределенности отдельных базовых событий в неопределенность общих результатов;

e) регистрацию результатов с их границами неопределенности, включая понимание того, какие источники неопределенности являются критическими для результатов.

6.3.9 Задача 8 — анализ чувствительности

Анализ чувствительности — это вид анализа неопределенности, который фокусируется на оценке влияния изменений (из-за неопределенности) в допущениях, моделировании, физических параметрах

и базовых событиях. Такой анализ часто проводят в рамках PRA, чтобы указать те аналитические входы или элементы, изменение значения которых вызывает наибольшие изменения в частичных или окончательных результатах риска. Анализ чувствительности также используется для оценки чувствительности результатов PRA к зависимостям между отказами базовых событий.

Задача 8 включает:

a) составление списка допущений, касающихся критериев успешного целевого применения космической системы, структуры, системы и компонентов, моделирования и физических параметров. Кроме того, определение тех структур, систем и компонентов, содержащихся в единых последовательностях опасных событий (минимальные наборы разрезов), имеющих общее свойство, которое может сделать их восприимчивыми к зависимым отказам;

b) систематическое и независимое варьирование критериев успеха, моделирования и значений показателей, а также изменение моделей PRA и данных путем соответствующей корректировки последовательности событий [дерева (деревьев) событий] и моделей отказа событий [дерева (деревьев) отказов] для допущений. Переоценка общей модели PRA на предмет изменений в опасной последовательности, ранжировании и количественных результатах риска;

c) для потенциально зависимых структур, систем и компонентов в рамках одного множества вырезок событий объединение их в одно базовое событие и присвоение ему наивысшей вероятности среди связанных событий. Независимая переоценка совокупной модели PRA на предмет изменений, происходящих в опасных последовательностях, ранжировании и количественных результатах риска от каждого скорректированного множества вырезок событий.

6.3.10 Задача 9 — ранжирование

В некоторых случаях применения PRA используются специальные методы для определения ведущих, или доминирующих, составляющих риска в опасных последовательностях или сценариях. Ранжирование этих ведущих, или доминирующих, составляющих в порядке убывания важности называется ранжированием по важности. Процесс ранжирования обычно выполняется с использованием последовательности событий [дерева (деревьев) событий] и моделей отказов событий [дерева (деревьев) отказов]. Существует несколько количественных показателей важности, которые обычно определяют изменение количественного риска (вероятности) в связи с изменением вероятности базового события или измеряют вклад базового события в совокупный риск. Некоторые из этих количественных показателей важности включают показатели Фюсселя-Везели (F-V, Fussell-Vesely), значимость снижения риска (RRW — risk reduction worth) и значимость достижения риска (RAW — risk achievement worth).

Задача 9 включает:

a) идентификацию основных составляющих риска;

b) оценку совокупного риска по выбранным мерам важности и соответствующее ранжирование отдельных опасных сценариев и базовых событий;

c) определение вклада в совокупный риск и неопределенность от этих опасных последовательностей и базовых событий.

6.3.11 Анализ данных

Анализ данных относится к процессу сбора и анализа информации и данных. Сбор и анализ данных происходят параллельно или совместно с девятью задачами PRA, описанными выше, поэтому в настоящем стандарте они не рассматриваются как отдельная задача. Одним из направлений использования анализа данных в PRA является оценка различных параметров входных событий и базовых событий, используемых в моделях PRA. Эти параметры обычно собирают в базу данных и используют для получения вероятностей отказов структур, систем и компонентов, частот входных событий, вероятностей отказов по причине действий персонала и общих факторов. В случаях, когда отсутствуют статистически значимые данные для оценки параметров PRA, аналитику могут потребоваться экспертная оценка и выводы.

Анализ данных PRA включает в себя следующие действия (но не ограничивается ими):

a) идентификацию данных, необходимых для входных событий и базовых событий в модели PRA;

b) сбор достоверной информации о событиях на основе объективных данных (результатов измерений или наблюдений в процессе испытаний и/или экспериментов), относительно объективных данных (экстраполяции на основе общих данных, данных для аналогичных объектов или физических моделей) и субъективных данных (экспертных оценок специалистов в исследуемых областях);

c) оценку вероятностей событий с помощью статистических методов и разработку распределений неопределенности;

d) разработку базы данных PRA, содержащей собранную информацию и данные, оценки параметров и вероятностей, включая неопределенности.

7 Экспертиза

7.1 Общие положения

Для повышения качества и достоверности PRA следует проводить внутренние и внешние экспертные оценки. В целом эти экспертизы направлены на оценку адекватности методов, информации, источников, суждений и предположений, а также на их применение к оцениваемому проекту и достижению поставленной(ых) цели(ей).

Целью проведения экспертных оценок является проверка правильности применения методологии и точности результатов анализа. Экспертные оценки должны проводиться для всех методов PRA.

7.2 Внутренняя экспертиза

Внутренние экспертные оценки проводят члены группы, состоящей из экспертов по предметам, для перекрестной проверки моделей и результатов. Эти экспертные оценки также включают в себя изучение и обсуждение моделей и результатов с наиболее сведущим в оцениваемых системах персоналом, включая проектировщиков, строителей и операторов.

7.3 Внешняя экспертиза

Этот вид экспертизы проводят независимые эксперты, т. е. люди, которые не участвуют в исследовании и не заинтересованы в нем, но обладают возможностями, превосходящими возможности лиц, проводивших исследование. Компетентность экспертов должна охватывать весь диапазон дисциплин, необходимых для проведения исследования, также они должны иметь соответствующий опыт.

Следует рассмотреть возможность использования коллегиальной экспертной оценки. Процесс коллегиальной экспертной оценки начинается на ранних этапах и идет параллельно с разработкой и реализацией проекта, предполагая частые, периодические контакты и взаимодействие экспертов с группой PRA. Этот тип экспертной оценки проводится для того, чтобы выявить проблемы и разработать рекомендации по корректирующим действиям на ранних этапах PRA, вместо того чтобы начинать проводить экспертную оценку, когда оценка PRA практически завершена. При таком подходе может снижаться степень независимости при проведении экспертной оценки, однако, скорее всего, его реализация приведет к тому, что PRA будет выполняться корректно с первого раза, что позволит избежать затрат времени и ресурсов на исправление проблем в конце проекта.

8 Отчет о вероятностной оценке риска. Требования к данным

В таблице 1 приведены требования к содержанию отчета о PRA. Отчет о PRA должен быть составлен в соответствии с данными, приведенными в указанной таблице. Отчет о PRA (нарушения) безопасности может быть объединен с отчетом об анализе опасностей.

Таблица 1 — Содержание отчета о PRA

Наименование раздела	Содержание
Титульный лист	Титульный лист должен содержать: - наименование документа; - номер документа и дату выпуска; - ФИО авторов или соавторов; - подписи ответственных лиц
Записи об изменении документа	Записи об изменении документа должны быть составлены в соответствии с требованиями менеджмента конфигурации проекта
Содержание	Наименования разделов отчета
Введение/область применения/аннотация	Этот раздел должен обеспечить краткое введение к отчету, описание его области применения и обзор основных результатов

Окончание таблицы 1

Наименование раздела	Содержание
Нормативные ссылки	Раздел должен содержать перечень всех нормативных и ссылочных документов, примененных в отчете
Термины, определения и сокращения	Должны быть приведены термины, определения и сокращения. Если они относятся не только к отчету, то они могут быть применены и в других документах
Область применения, основная задача и система	В разделе должны быть описаны область применения, основная задача проекта и система (системы) или ее часть, включенная в анализ
Требования	В разделе должно быть приведено краткое изложение требований к рассматриваемым системам и к выполнению оценки, включая значимость последствий и ранжирование вероятностей сценария
Предположения	В разделе должно быть приведено описание всех предположений, сделанных при выполнении оценки, включая, при необходимости, все ограничения на выполнение оценки (например, при рассмотрении не всех выполненных задач)
Описание системы и функций	В разделе должно быть приведено описание систем и их функций в деталях, достаточных для моделирования и получения необходимых результатов оценки
Описание методов, моделей и аналитических методик[1)]	В разделе должно быть приведено описание методов и моделей, используемых при выполнении анализа, включая, если применимо, аналитические методики оценки реакции систем и количественной оценки последствий
Анализ данных[2)]	В этом разделе должно быть приведено описание данных, методов сокращения данных и моделей неопределенности, используемых при оценке
Краткое изложение результатов и рекомендаций	В разделе должны быть приведены результаты оценки и рекомендации по результатам их анализа

---

1) При формировании указанного раздела отчета также применяют положения ГОСТ Р 58771—2019 (в части выбора технологий вероятностной оценки риска — раздел 7, в части описания технологий — Б.2.3, Б.4.4, Б.5.2, Б.5.3, Б.5.5 — Б.5.10, Б.5.13, Б.5.14, Б.6.2, Б.7.2, Б.7.3, Б.8.2, Б.8.3, Б.8.5, Б.9.4 приложения Б) и иные документы по стандартизации, к области применения которых относится указанный объект.

2) Данные, используемые при количественной оценке риска, должны выражаться через измеряемые параметры (величины). При формировании указанного раздела отчета также может быть учтена суммарная совокупность измеряемых параметров (величин), в том числе в процентном отношении.

Для оценки риска в большинстве случаев рекомендуется использовать результаты не менее трех предыдущих испытаний.

Приложение А
(справочное)

Пример определений категорий удельной стоимости/критичности для проекта в области космических систем

Таблица А.1 — Пример определений категорий удельной стоимости/критичности для проекта в области космических систем

Категория 5. Высокий уровень III	Категория 4. Высокий уровень II	Категория 3. Высокий уровень I	Категория 2. Средний уровень	Категория 1. Низкий уровень
Оборонные космические аппараты. Пусковые установки. Ракеты большой дальности. Космические аппараты с ядерным двигателем. Аппаратные/программные компоненты для завершения полета. Оборудование, излучающее радиацию/высокую энергию. Пилотируемые космические аппараты и пилотируемые космические комплексы	Коммерческие космические аппараты/спутники связи. Экспериментальные пилотируемые космические аппараты. Ракеты малой дальности. Пилотируемые космические аппараты на низкой околоземной орбите. Критически важные для безопасности человека или окружающей среды аппаратные/программные компоненты. Станции управления военными спутниками. Устойчивая к радиации электроника космических аппаратов. Взрывные устройства космических аппаратов	Научно-исследовательские космические аппараты. Малые спутники. Микроспутники CubeSats (угроза обломков). Критически важные для безопасности аппаратные и программные компоненты, не относящиеся к человеку и окружающей среде. Станции управления коммерческими спутниками. Военные компьютеры/периферийные устройства. Электроника космических аппаратов военного класса. Конструкции и механизмы космических аппаратов. Сосуды под давлением для космических аппаратов. Аппараты для посадки на комету/планету	Микроспутники CubeSats (угроза, не связанная с обломками). Электроника космических аппаратов промышленного класса. Промышленные компьютеры/периферийные устройства. Оборудование для космических экспериментов. Аппаратное/программное обеспечение для мониторинга состояния космического аппарата. Компьютерные операционные системы. Прототипы систем и компонентов космических аппаратов. Спутниковые станции ретрансляции данных	Моторизованные/ручные инструменты для сборки космических аппаратов. Изоляционные материалы космических аппаратов. Прикладные компьютерные программы

Приложение В
(справочное)

Руководство по адаптации процесса PRA на основе возможностей

В.1 Действия процесса PRA на уровне возможностей 1

В.1.1 Авторизация функции PRA подрядчика и возложение на него ответственности и полномочий за выполнение требований PRA, предусмотренных настоящим стандартом, условиями контракта и командными средствами поставщика на уровне предприятия. По мере необходимости следует санкционировать внедрение адаптированного процесса PRA надлежащим образом обученным персоналом:

- назначение квалифицированного руководства и технических специалистов для проведения PRA и предоставление им инструментов, необходимых для планирования и реализации экономически эффективного процесса PRA;
- использование проверенных методов для выявления, оценки и устранения или управления приемлемыми рисками невыполнения проекта и безопасности системы.

В.1.2 Выявление применимых требований к PRA. Выявленные требования к PRA должны соответствовать настоящему стандарту и условиям контракта. Поставщик должен передать требования к PRA всем зависимым от него поставщикам, которые вносят вклад в PRA. Основные задачи PRA заключаются в следующем:

- определение целей и подхода;
- изучение системы;
- оценка входного события;
- моделирование сценариев;
- моделирование отказов;
- количественная оценка;
- анализ неопределенностей;
- анализ чувствительности (с использованием технической оценки);
- ранжирование рисков (с использованием технической оценки).

В.1.3 Документирование внутреннего утвержденного плана PRA, который соответствует настоящему стандарту, условиям контракта и командным средствам поставщика на уровне предприятия.

В.1.4 Координация деятельности по PRA и элементов данных с зависимыми поставщиками.

В.1.5 Применение передовой инженерной практики для выполнения основных задач PRA.

В.1.6 Реализация процесса качественной оценки риска, соответствующего настоящему стандарту и ИСО 17666.

В.1.7 Использование формальных и неформальных методов для проверки выполнения требований к PRA. Формальные методы проверки предполагают рассмотрение и согласование с заказчиком. Проверка снижения рисков, связанных с опасными материалами, обычно проводится формальным методом. Неформальные методы проверки предполагают проверку и согласование только со стороны внутреннего руководства.

В.1.8 Документирование результатов выполнения плана PRA в протоколе PRA.

Примечание — Протокол PRA обновляют «по требованию» или «по необходимости». Обновления «по требованию» инициируются запланированными событиями, например требуемыми по контракту сроками поставки. Обновления «по необходимости» инициируются незапланированными событиями, например изменениями, внесенными в систему или проект, которые влияют на целостность данных в текущем протоколе.

В.2 Действия процесса PRA на уровне возможностей 2

В.2.1 Процесс PRA уровня возможностей 2 содержит все виды деятельности, предусмотренные процессом PRA на уровне возможностей 1, а также следующие изменения.

В.2.2 Замена восьмого и девятого элементов списка пункта В.1.2 на следующие:

- анализ чувствительности (с использованием методов руководства);
- ранжирование рисков (с использованием методов руководства).

В.2.3 Замена пункта В.1.3 на «Документирование официально утвержденного плана PRA, который соответствует настоящему стандарту, условиям контракта и командным средствам поставщика на уровне предприятия. Следует обратить внимание, что официальное утверждение включает в себя рассмотрение и согласование с заказчиком».

В.2.4 Мониторинг деятельности по PRA зависимых поставщиков.

В.2.5 Установление технических показателей эффективности для отслеживания и отчетности о результатах процесса PRA.

В.3 Действия процесса PRA на уровне возможностей 3

В.3.1 Процесс PRA уровня возможностей 3 содержит все виды деятельности, предусмотренные процессом PRA на уровнях возможностей 1 и 2, а также следующие изменения.

В.3.2 Замена восьмого и девятого элементов списка пункта В.1.2 на следующие:

- анализ чувствительности (с использованием методов анализа сходства);
- ранжирование рисков (с использованием методов анализа сходства).

В.3.3 Оценка требований PRA с использованием анализа опасности системных требований или эквивалентной методологии для выявления противоречивых требований, нечетких требований, фальсификации требований и других нежелательных требований.

Следует отметить, что противоречивые требования к логистической поддержке ранжируют с учетом следующего:

1) требования к безопасности системы;
2) требования к доступности;
3) требования к надежности;
4) требования к ремонтопригодности и пригодности к испытаниям.

В.3.4 Замена пункта В.1.6 на «Реализация процесса менеджмента риска количественной поддержки, соответствующего настоящему стандарту и ИСО 17666».

В.3.5 Создание, использование и поддержание системы базы данных проекта по PRA, которая:

1) обеспечивает бесперебойное взаимодействие между всеми видами деятельности по PRA;
2) отслеживает все данные PRA;
3) имеет процедуры управления изменениями данных и их отслеживания;
4) может обрабатывать протоколы PRA.

В.3.6 Гарантия того, что все заинтересованные в снижении системного риска стороны получают протоколы PRA.

В.3.7 Сбор, анализ и использование накопленного опыта PRA, если это применимо.

В.3.8 Оценивание всех аспектов процесса PRA для выявления новых извлеченных уроков PRA, если это применимо.

В.4 Действия процесса PRA на уровне возможностей 4

В.4.1 Процесс PRA уровня возможностей 4 содержит все виды деятельности, предусмотренные процессом PRA на уровнях возможностей 1, 2 и 3, а также следующие изменения.

В.4.2 Замена восьмого и девятого элементов списка пункта В.1.2 на следующие:

- анализ чувствительности (с использованием данных испытаний или моделирования);
- ранжирование рисков (с использованием данных испытаний или моделирования).

В.4.3 Замена пункта В.1.4 на «Надзор за деятельностью по PRA зависимых поставщиков для обеспечения заранее определенных форматов данных PRA, которые облегчают их интеграцию в модель (модели) поставщика».

В.4.4 Оценивание готовности продуктов данных PRA.

В.4.5 Использование проверенных компьютеризированных инструментов PRA, которые легко интегрируются в систему базы данных PRA проекта.

В.4.6 Создание внутренних каналов для обмена опытом, полученным в ходе PRA, с другими проектами поставщика.

В.4.7 Установление минимальных квалификационных требований для лиц, осуществляющих деятельность по PRA, требующую большого опыта или обучения.

В.4.8 Замена пункта В.1.6 на «Реализация процесса количественного менеджмента риска, который отвечает требованиям настоящего стандарта и ИСО 17666 и содержит следующее:

- мониторинг всех выявленных остаточных рисков;
- непрерывный менеджмент рисков, критически важных для целевого применения космической системы и безопасности объектов».

В.5 Действия процесса PRA на уровне возможностей 5

В.5.1 Процесс PRA уровня возможностей 5 содержит все виды деятельности, предусмотренные процессом PRA на уровнях возможностей 1, 2, 3 и 4, а также следующие изменения.

В.5.2 Замена восьмого и девятого элементов списка пункта В.1.2 на следующие:

- анализ чувствительности (с использованием демонстрационных данных);
- ранжирование рисков (с использованием демонстрационных данных).

В.5.3 Проведение официальных экспертных оценок для периодической оценки процесса PRA.

В.5.4 Постоянное совершенствование процесса PRA посредством:

- внедрения внутренних процессов, способствующих тому, чтобы отдельные лица и команды инициативно выявляли и оценивали риски невыполнения проекта и риски (нарушения) безопасности системы;
- периодического обучения руководства и технических специалистов надлежащему использованию компьютеризированных инструментов PRA и ознакомления их с новыми извлеченными уроками PRA.

В.5.5 Создание внешних каналов для обмена уроками, полученными в ходе PRA, с государственными и частными организациями, включая других поставщиков.

B.6 Реализация мероприятий по PRA на основе возможностей на протяжении всего жизненного цикла системы по мере необходимости

На протяжении всего жизненного цикла космических систем осуществляются конкретные мероприятия по выявлению и устранению недопустимых критически важных для целевого применения космической системы и безопасности рисков или их менеджмент. В таблице B.1 приведен пример адаптации процесса PRA на протяжении жизненного цикла космических систем.

Таблица B.1 — Пример адаптации процесса вероятностной оценки риска на протяжении жизненного цикла космических систем

Уровень удельной стоимости/ критичности для выполнения проекта в области космических систем	Стадия жизненного цикла				
	Стадия концептуального определения систем	Стадия чернового проектирования	Стадия детального проектирования	Стадия изготовления, сборки, интеграции и испытаний	Стадия эксплуатации и поддержки
Низкий	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 1 (*)
Средний	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 2 (*)
Высокий I	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 3	Процесс PRA на уровне возможностей 3	Процесс PRA на уровне возможностей 3 (*)
Высокий II	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 3	Процесс PRA на уровне возможностей 4	Процесс PRA на уровне возможностей 4 (*)
Высокий III	Процесс PRA на уровне возможностей 1	Процесс PRA на уровне возможностей 2	Процесс PRA на уровне возможностей 3	Процесс PRA на уровне возможностей 4	Процесс PRA на уровне возможностей 5 (*)

Примечание — (*) указывает, что уровень возможностей процесса применяется только к изменениям, которые происходят на этапе жизненного цикла космической системы.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 17666	IDT	ГОСТ Р ИСО 17666—2021 «Менеджмент риска. Космические системы»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT— идентичный стандарт.

Библиография

[1] ISO 14620-2:2011, Space systems — Safety requirements — Part 2: Launch site operations (Системы космические. Требования безопасности. Часть 2. Работа стартовых площадок)

[2] ISO 16192, Space systems — Experience gained in space projects (lessons learned) — Principles and guidelines [Системы космические. Опыт, накопленный в космических проектах (извлеченные уроки). Принципы и руководство]

[3] ISO/TS 18667, Space systems — Capability-based Safety, Dependability, and Quality Assurance (SD&QA) programme management [Системы космические. Менеджмент программ по безопасности, надежности и обеспечению качества (SD&QA) на основе мандатов]

[4] IEC 60300-3-9, Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems (Менеджмент надежности. Часть 3. Руководство по применению. Раздел 9. Анализ рисков технологических систем)

УДК 658:562.014:006.354 ОКС 49.140

Ключевые слова: менеджмент риска, оценка риска, методы оценки риска, анализ опасностей, анализ сценариев, PRA

Редактор *М.В. Митрофанова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 21.08.2024. Подписано в печать 29.08.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,77.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru