ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ

Анализ риска технологических систем

Издание официальное

БЗ 6—2002/90

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Научно-исследовательским институтом контроля и диагностики технических систем (АО НИЦ КД)

ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Основополагающие общетехнические стандарты. Оценка эффективности и управление рисками»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 7 июня 2002 г. № 236-ст

3 Настоящий стандарт гармонизирован с международным стандартом МЭК 60300-3-9:1995 «Dependability Management — Part 3: Application guide — section 9: Risk analysis of technological systems» — «Управление надежностью. Часть. 3. Руководство по применению. Раздел 9. Анализ риска технологических систем»

4 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Процесс управления риском охватывает различные аспекты работы с риском, от идентификации и анализа риска до оценки его допустимости и определения потенциальных возможностей снижения риска посредством выбора, реализации и контроля соответствующих управляющих действий.

Анализ риска представляет собой структурированный процесс, целью которого является определение как вероятности, так и размеров неблагоприятных последствий исследуемого действия, объекта или системы. В настоящем стандарте в качестве неблагоприятных последствий рассматривается вред, наносимый людям, имуществу или окружающей среде.

Посредством проведения анализа риска предпринимаются попытки ответить на три основных вопроса:

что может выйти из строя (идентификация опасности);

с какой вероятностью это может произойти (анализ частоты);

каковы последствия этого события (анализ последствий).

Настоящий стандарт отражает современный практический опыт, накопленный в области выбора и применения методов анализа риска.

Настоящий стандарт носит общий характер, он применим для многих отраслей и типов технических систем. Для конкретных отраслей могут существовать стандарты, которые устанавливают методологии оценки и анализа риска для определенных областей применения. Если требования этих стандартов не хуже требований настоящего стандарта, то их применение является предпочтительным.

Настоящий стандарт охватывает лишь часть вопросов по оценке и анализу риска. Действия по оценке риска и управлению рисками являются предметом других стандартов. Настоящий стандарт основан на концепциях, установленных в документах [1]—[3], приведенных в библиографии, и других стандартах. Существуют многочисленные примеры ситуаций, когда данные документы не являются в полной мере совместимыми, либо когда они применимы в отдельной отрасли. В таких случаях может использоваться либо один из имеющихся в настоящем стандарте подходов, либо подход более общего характера.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ

Анализ риска технологических систем

Dependability management.
Risk analysis of technological systems

Дата введения 2003—09—01

1 Область применения

Настоящий стандарт устанавливает руководящие указания по выбору и реализации методов анализа риска, главным образом для оценки риска технологических систем. Целью настоящего стандарта является обеспечение качества при планировании и выполнении анализа риска, а также установление рекомендаций по представлению полученных результатов и выводов.

Руководящие указания настоящего стандарта включают: концепции анализа риска, процесс анализа риска, методы анализа риска.

Настоящий стандарт применим в качестве:

- руководства по планированию, выполнению и документальному обоснованию анализа риска;
- основы для назначения требований к качеству анализа риска (особенно в тех случаях, когда анализ риска проводится сторонними консультантами);
- основы для оценки проведенного анализа риска.

Анализ риска, осуществляемый в соответствии с настоящим стандартом, является элементом управления риском.

Примечание — Настоящий стандарт не предусматривает определения критериев для установления потребности в анализе риска, то есть не определяет тип метода анализа риска, который необходим для данной ситуации, а также не затрагивает гарантийных, страховых, правовых или финансовых аспектов возможных видов опасности.

2 Определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

2.1 **вред (harm):** Физический ущерб или урон здоровью, имуществу или окружающей среде.

2.2 **опасность (hazard):** Источник потенциального вреда или ситуация с потенциальной возможностью нанесения вреда.

2.3 **опасное событие (hazardous event):** Событие, которое может причинить вред.

2.4 **идентификация опасности (hazard identification):** Процесс осознания того, что опасность существует, и определения ее характерных черт.

2.5 **риск (risk):** Сочетание вероятности события и его последствий.

Примечание — Термин «риск» обычно используется тогда, когда существует хотя бы возможность негативных последствий.

2.6 **анализ риска (risk analysis):** Систематическое использование информации для определения источников и количественной оценки риска.

Примечание — Анализ риска обеспечивает базу для оценивания риска, мероприятий по снижению риска и принятия риска.

Издание официальное

2.7 **оценка риска (risk assessment):** Общий процесс анализа риска и оценивания риска. (см. рисунок 1)

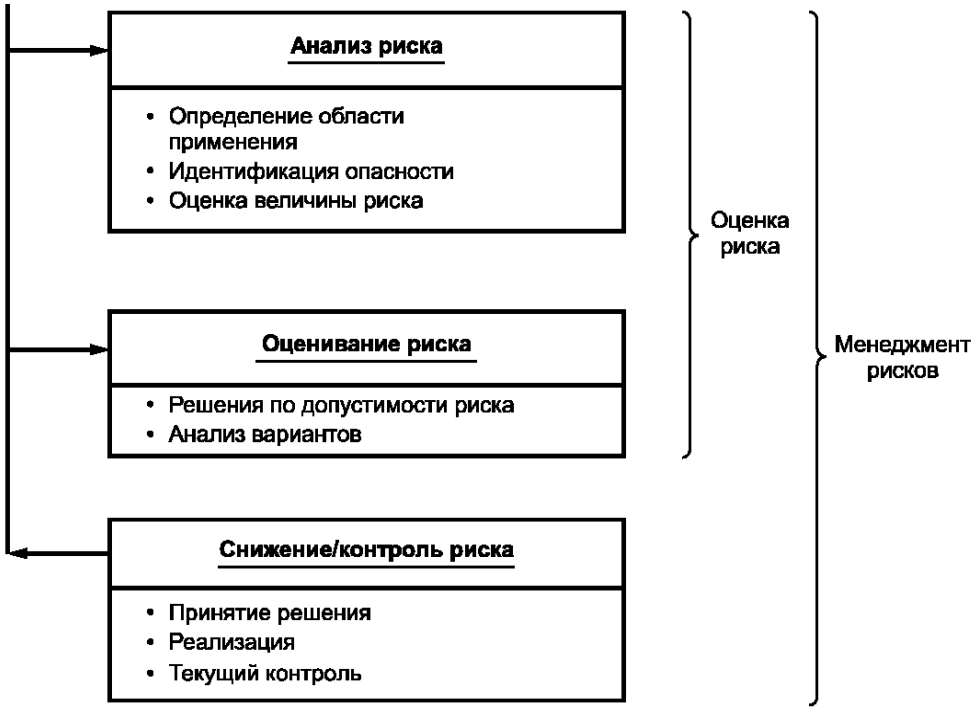


Рисунок 1 — Соотношения между анализом риска и другими действиями по управлению риском

2.8 **управление риском (risk control):** Действия, осуществляемые для выполнения решений в рамках менеджмента рисков.

Примечание — Управление риском может включать мониторинг, переоценивание и соответствие принятым решениям.

2.9 **оценка величины риска (risk estimation):** Процесс присвоения значений вероятности и последствий риска.

Примечание — Оценка величины риска может рассматривать стоимость, выгоды, озабоченность участвующих сторон и другие переменные, рассматриваемые при оценивании риска.

2.10 **оценивание риска (risk evaluation):** Процесс сравнения оцененного риска с данными критериями риска с целью определения значимости риска.

Примечание — Оценивание риска может быть использовано для содействия решениям по принятию или обработке риска.

2.11 **менеджмент риска (risk management):** Скоординированные действия по руководству и управлению организацией в отношении рисков.

Примечание — Обычно менеджмент риска включает оценку рисков, обработку рисков, принятие рисков и коммуникацию рисков.

2.12 **система (system):** Составной объект любого уровня сложности, который может включать персонал, процедуры, материалы, инструменты, оборудование, средства обслуживания, программное обеспечение.

3 Концепции анализа риска

3.1 Цель и основные концепции анализа риска

Риск присутствует в любой деятельности человека. Он может относиться к здоровью и безопасности (учитывая, например, как немедленные, так и долгосрочные последствия для здоровья от воздействия токсичных химических продуктов). Риск может быть экономическим, например,

приводящим к уничтожению оборудования и продукции вследствие пожаров, взрывов или других аварий. Он может учитывать неблагоприятные воздействия на окружающую среду. Задачей управления рисками является контроль, предотвращение или сокращение гибели людей, снижение заболеваемости, снижение ущерба, урона имуществу и логически вытекающих потерь, а также предотвращение неблагоприятного воздействия на окружающую среду.

Для повышения эффективности управления рисками необходимо проводить предварительный анализ риска, включающий:

а) идентификацию риска и определение подходов к решению связанных с ним проблем;

б) использование объективной информации при принятии решений;

в) удовлетворение регламентированных требований к риску.

Результаты анализа риска могут использоваться специалистом, принимающим решение при оценке допустимости риска, а также при выборе между потенциальными мерами по снижению или устранению риска. С точки зрения специалиста, принимающего решение, к основным достоинствам анализа риска относятся:

а) систематическая идентификация потенциальных опасностей;

б) систематическая идентификация возможных видов отказов;

в) количественные оценки или ранжирование рисков;

г) оценка надежности возможных модификаций системы для снижения риска и достижения предпочтительных уровней ее надежности;

д) выявление факторов, обуславливающих риск, и слабых звеньев в системе;

е) более глубокое понимание устройства и функционирования системы;

ж) сопоставление риска исследуемой системы с рисками альтернативных систем или технологий;

и) идентификация и сопоставление рисков и неопределенностей;

к) помощь в установлении приоритетов при совершенствовании санитарных требований и норм;

л) формирование базы для рациональной организации профилактического обслуживания, ремонта и контроля;

м) обеспечение возможности поставарийного расследования и мер по предупреждению аварий;

н) возможность выбора мер и приемов по обеспечению снижения риска.

Все эти факторы играют важную роль в эффективном управлении рисками независимо от того, какие задачи рассматриваются (охрана здоровья, безопасность, предотвращение экономических потерь, обеспечение выполнения требований постановлений правительства и т. п.).

Анализ может охватывать такие области специальных знаний, как:

а) системный анализ;

б) вероятность и статистика;

в) химическая технология, машиностроение, электротехника, строительная техника или ядерная техника;

г) физические, химические или биологические науки;

д) медицинские науки, в том числе токсикология и эпидемиология;

е) общественные науки, в том числе экономика, психология и социология;

ж) влияние человеческого фактора, эргономика и наука управления.

3.2 Управление рисками и распределение рисков по категориям

Анализ риска является частью оценки риска и процесса управления риском, показанного на рисунке 1, и состоит из определения области применения, идентификации опасности и оценки величины риска.

Опасности могут быть отнесены к следующим четырем основным категориям:

а) природные опасности (наводнения, землетрясения, ураганы, молния и т. д.);

б) технические опасности, источниками которых являются промышленное оборудование, сооружения, транспортные системы, потребительская продукция, пестициды, гербициды, фармацевтические препараты и т. п.;

в) социальные опасности, источниками которых являются вооруженное нападение, война, диверсия, инфекционное заболевание и т. д.;

г) опасности, связанные с укладом жизни (злоупотребление наркотиками, алкоголь, курение и т. д.).

Очевидно, что данные категории не являются взаимоисключающими. Так при анализе технических опасностей часто бывает необходимо учитывать влияние факторов из других категорий (в особенности природных опасностей) и других систем в качестве части анализа риска.

Риск также может быть классифицирован, исходя из характера возможных последствий. Например, характер последствий может быть:

а) индивидуальным (воздействие на отдельных людей);

б) профессиональным (воздействие на работающих);

в) социальным (общее воздействие на сообщество людей);

г) приводящим к имущественному урону и экономическим потерям (нарушения деловой деятельности, штрафы и т. д.);

е) касающимся окружающей среды (воздействие на землю, воздух, воду, растительный, животный мир и культурное наследие).

Общей задачей анализа риска является обоснование решений, касающихся риска. Эти решения могут приниматься как часть более крупного процесса управления рисками посредством сопоставления результатов анализа риска с критериями допустимого риска. Во многих ситуациях возникает необходимость оценивания преимуществ того или иного решения. В целом назначение критериев допустимого риска является достаточно сложной задачей, особенно в социальной, экономической и политической областях, и находится вне сферы рассмотрения настоящего стандарта.

3.3 Применение анализа риска на различных стадиях жизненного цикла

В настоящем подразделе перечислены некоторые конкретные цели анализа риска, относящиеся к различным стадиям жизненного цикла опасных систем, оборудования или изделий:

а) Стадия проектирования:

1) выявление главных источников риска и предполагаемых факторов, существенно влияющих на риск;

2) предоставление исходных данных для оценки конструкции в целом;

3) определение и оценка возможных мер безопасности, закладываемых в конструкцию;

4) предоставление исходных данных для оценки потенциально опасных действий, оборудования или систем;

5) обеспечение соответствующей информацией при проведении опытно-конструкторских работ, ориентированных на нормальные и чрезвычайные условия;

6) оценка риска с учетом регламентов и других требований;

7) оценка альтернативных конструктивных решений.

б) Стадии изготовления, монтажа, эксплуатации и технического обслуживания:

1) контроль и оценка данных эксплуатации с целью сопоставления фактических показателей работы с соответствующими требованиями;

2) обеспечение исходными данными процесса разработки методик эксплуатации, технического обслуживания/контроля и действий в чрезвычайных ситуациях;

3) корректировка информации об основных источниках риска и влияющих факторах;

4) предоставление информации по значимости риска для принятия оперативных решений;

5) определение влияния изменений в организационной структуре, производстве, процедурах эксплуатации и компонентах системы;

6) подготовка персонала.

в) Стадия демонтажа, прекращения эксплуатации:

1) оценка риска, связанного с прекращением функционирования системы, и обеспечение возможности выполнения соответствующих требований;

2) обеспечение исходными данными процесса прекращения функционирования системы и ее демонтажа.

4 Процесс анализа риска

4.1 Общие положения

Для повышения эффективности и объективности анализа риска и обеспечения сопоставимости с другими результатами по анализу риска необходимо соблюдать следующие общие правила. Процесс анализа риска должен осуществляться в соответствии со следующими этапами:

а) определение области применения;

б) идентификация опасности и предварительная оценка последствий;

в) оценка величины риска;

г) проверка результатов анализа;

д) документальное обоснование;

е) корректировка результатов анализа с учетом последних данных.

Данный процесс показан на рисунке 2. Оценка риска включает проведение анализа частот и анализа последствий. Несмотря на то, что на рисунке 2 документация изображена в качестве отдельного блока, она разрабатывается на каждой стадии процесса. В зависимости от области применения рассматриваются лишь определенные элементы представленного процесса. Например, в некоторых случаях может оказаться, что нет необходимости выходить за рамки исходного анализа опасности и последствий.

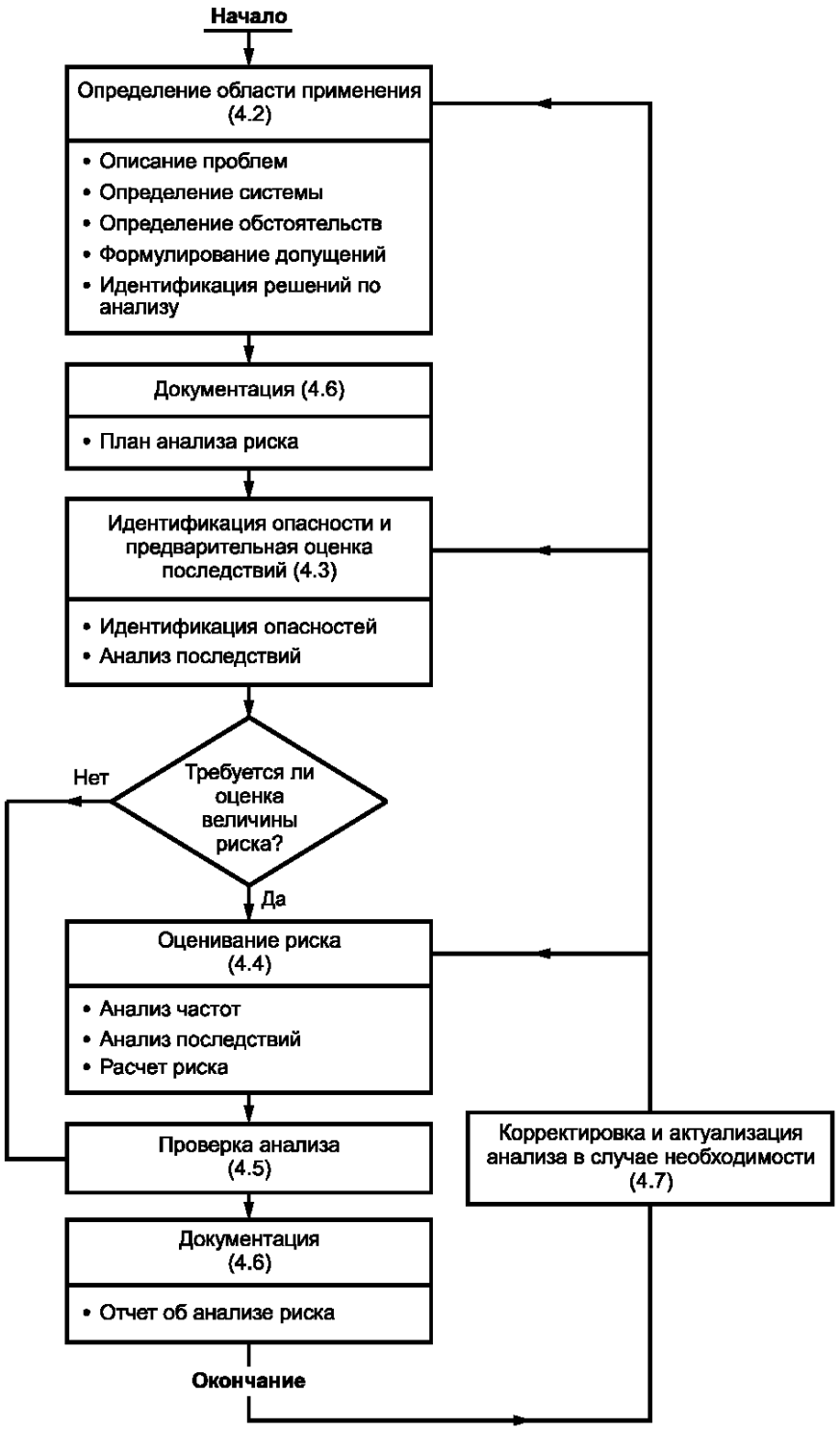


Рисунок 2 — Процесс анализа риска (раздел 4)

Необходимым требованием является скрупулезное знание системы и используемых методов анализа. В том случае, если имеются результаты анализа риска для похожей системы, они могут быть использованы в качестве справочного материала. При этом необходимо доказать, что процессы являются похожими, и что внесение изменений не вносит существенных различий в результаты. Выводы должны основываться на систематической оценке изменений и на том, каким образом они могут влиять на существующие опасности.

4.1.1 Персонал для проведения анализа риска

Аналитики, участвующие в анализе риска, должны быть достаточно компетентными. Многие системы слишком сложны для работы одного человека, поэтому для выполнения анализа требуется группа аналитиков.

Отдельное лицо или рабочая группа должны быть ознакомлены с методами, используемыми для анализа риска, и должны располагать достаточными знаниями о рассматриваемом предмете. При необходимости для проведения анализа должны быть представлены и использованы другие необходимые сведения. Заключение специалистов рабочей группы должно быть документально зафиксировано.

4.2 Определение области применения

Для выработки плана анализа риска область применения анализа риска должна быть определена и документально установлена. Определение области применения анализа риска должно включать в себя следующие этапы:

а) Описание оснований и/или проблем, повлекших проведение анализа риска. Это предусматривает:

1) формулировку задач анализа риска, основанных на внушающих тревогу идентифицированных потенциальных опасностях;

2) определение критериев работоспособности/отказа системы. Основными потенциально опасными моментами могут быть нежелательные состояния системы, например, отказ системы, выброс ядовитого материала и т. п.

б) Описание исследуемой системы.

Это должно включать в себя:

1) общее описание системы;

2) определение границ и областей контакта со смежными системами;

3) описание условий окружающей среды;

4) выделение видов энергии, материалов и информации, превышающих допустимые границы;

5) определение рабочих условий и состояний системы, на которые распространяется анализ риска, и соответствующие ограничения.

в) Установление источников, предоставляющих подробную информацию о всех технических, связанных с окружающей средой, правовых, организационных и человеческих факторах, имеющих отношение к анализируемым действиям и проблеме. В частности, должны быть описаны любые обстоятельства, касающиеся безопасности.

г) Описание используемых предположений и ограничивающих условий при проведении анализа.

д) Разработка формулировок решений, которые могут быть приняты, описание требуемых выходных данных, полученных по результатам исследований и от лиц, принимающих решения.

Задача по определению области применения анализа риска должна предусматривать тщательное ознакомление с анализируемой системой. Одна из целей ознакомления — это определение источников и методов использования специализированной информации.

4.3 Идентификация опасности и предварительная оценка последствий

Для решения поставленной задачи должны быть идентифицированы опасности, являющиеся причиной риска, а также пути, по которым эти опасности могут реализовываться.

Известные опасности (возможно, имевшие место при предыдущих авариях) должны быть четко и точно определены. Для идентификации опасностей, не учитываемых ранее при проведении анализа, должны применяться формальные методы (см. 6.3.1).

Предварительную оценку значения идентифицированных опасностей необходимо выполнять, основываясь на анализе последствий и изучении их основных причин.

Предварительная оценка значения идентифицированных опасностей определяет выбор последующих действий:

а) принятие немедленных мер с целью исключения или уменьшения опасностей;

б) прекращение анализа, поскольку опасности или их последствия являются несущественными;

в) переход к оцениванию риска.

Исходные допущения и результаты должны быть документально зафиксированы (см. 4.6).

4.4 Оценка величины риска

В процессе оценки величины риска для выбора критического уровня анализируемых рисков должны исследоваться начальные события или обстоятельства, последовательность потенциально опасных событий, любые смягчающие факторы и характеристики, а также природа и частота возможных пагубных последствий идентифицированных опасностей. Эти критерии и меры должны распространяться на риски для людей, имущества и окружающей среды и должны включать значения неопределенностей оценок. Указанный процесс изложен в 4.4.1, 4.4.2 и 4.4.3. Методы анализа риска описаны в таблице 1.

Методы, используемые для оценки величины риска, обычно являются количественными, несмотря на то, что степень детализации при подготовке исходной информации зависит от конкретного применения (см. 6.2). Однако полный количественный анализ не всегда возможен из-за недостатка информации о системе или деятельности, подвергающейся анализу, отсутствия или недостатка данных об отказе (аварии), влиянии человеческого фактора и т. п. При таких обстоятельствах может оказаться эффективным сравнительное количественное или качественное ранжирование риска специалистами, хорошо информированными в данной области. В тех случаях, когда проводится качественное ранжирование, необходимо иметь четкое разъяснение всех используемых терминов и должно быть зафиксировано обоснование всех классификаций частот и последствий. В том случае, когда проводится полная количественная оценка величины риска, необходимо учитывать, что расчетные значения риска представляют собой оценки и следует позаботиться о том, чтобы их точность соответствовала точности используемых данных и аналитических методов.

Элементы процесса оценки величины риска являются общими для всех видов опасности. Прежде всего анализируются возможные причины опасности с целью определения частоты ее возникновения, продолжительности, а также характера (количественные характеристики, характеристики химического состава, характеристики выделения/использования и т. д.). В том случае, если анализу подвергается промышленное оборудование, в первую очередь проводится анализ частот, во вторую очередь анализу подвергаются последствия реализации опасности. В процессе анализа может возникнуть необходимость определения оценки вероятности опасности, вызывающей последствия, и проведения анализов последовательности обуславливающих событий.

4.4.1 Анализ частот

Анализ частот используется для оценки вероятности каждого нежелательного события, идентифицированного на стадии идентификации опасности. Для оценки частот происходящих событий обычно применяются следующие три подхода (см. 6.3.2.1):

а) использование имеющихся статистических данных (предыстория);

б) получение частот происходящих событий на основе аналитических или имитационных методов;

в) использование мнений экспертов.

Все эти технические приемы могут применяться по отдельности или совместно. Первые два подхода являются взаимодополняющими; каждый имеет сильные стороны там, где другой имеет слабые. Повсюду, где это возможно, должны применяться оба подхода. Таким образом, они могут использоваться для взаимных проверок. Это может служить повышению степени достоверности результатов. В тех случаях, когда данные подходы не могут использоваться либо являются недостаточными, рекомендуется привлекать мнения экспертов.

4.4.2 Анализ последствий

Анализ последствий используется для оценки вероятного воздействия, которое вызывается нежелательным событием.

Анализ последствий должен:

а) основываться на выбранных нежелательных событиях;

б) описывать любые последствия, являющиеся результатом нежелательных событий;

в) учитывать существующие меры, направленные на смягчение последствий, наряду со всеми соответствующими условиями, оказывающими влияние на последствия;

г) устанавливать критерии, используемые для полной идентификации последствий;

д) рассматривать и учитывать как немедленные последствия, так и те, которые могут проявиться по прошествии определенного периода времени, если это не противоречит сфере распространения исследований;

е) рассматривать и учитывать вторичные последствия, распространяющиеся на смежное оборудование и системы.

4.4.3 Вычисления

Риск должен выражаться в наиболее подходящих показателях. Некоторыми часто используемыми результатами вычислений являются:

а) прогнозируемая частота смертности или заболеваемости применительно к отдельному человеку (индивидуальный риск);

б) диаграммы частоты в зависимости от последствия (известные как кривые *F-N*, где *F* — частота; *N* — совокупное число людей, которым причинен вред определенного вида, либо совокупная стоимость ущерба) для социального риска;

в) статистически ожидаемый размер потерь от возникновения аварий, экономических затрат или урона для окружающей среды;

г) распределение риска с соответствующим уровнем ущерба, представленное в виде графика и указывающее уровни равного ущерба.

Необходимо установить, отражает ли полученная оценка риска уровень общего риска или является лишь его частью.

При расчете риска необходимо учитывать как продолжительность нежелательного события, так и вероятность того, что люди будут подвергаться его воздействию.

Данные, используемые для расчета уровней риска, должны соответствовать конкретному виду применения. Такого рода данные, по возможности, должны основываться на конкретных анализируемых обстоятельствах. Если таковые отсутствуют, должны использоваться данные общего характера, являющиеся характерными и представительными для данной ситуации, либо должна использоваться пользующаяся доверием экспертная оценка.

Данные должны собираться и группироваться в такой форме, которая способствовала бы удобному поиску информации для ее использования при анализе риска. Данные, которые более не соответствуют современному состоянию системы, должны быть выявлены и исключены из информации, используемой при анализе.

4.4.4 Неопределенности

Существует множество неопределенностей, связанных с оценкой риска. Понимание неопределенностей и вызывающих их причин необходимо для эффективной интерпретации значений риска. Анализ неопределенностей, связанных с используемыми данными, методами и моделями, применяемыми для оценки ожидаемого риска, играет существенную роль. Анализ неопределенностей предусматривает определение изменений и неточностей в результатах моделирования, которые являются следствием отклонения параметров и предположений, применяемых при построении модели. Областью, тесно связанной с анализом неопределенностей, является анализ чувствительности. Анализ чувствительности подразумевает определение изменений в реакции модели на отклонения отдельных параметров модели.

Оценка неопределенности состоит из преобразования неопределенности критических параметров модели в неопределенность результатов в соответствии с моделью риска. Требования к полноте и точности оценки риска должны быть сформулированы настолько полно, насколько это возможно. Там, где это возможно, должны быть выявлены источники неопределенности. Это относится как к неопределенностям данных, так и к неопределенностям модели. Должны быть точно определены те параметры, к которым чувствителен анализ.

4.5 Проверка анализа

Проверка анализа должна осуществляться людьми, не привлеченными к участию в анализе. Проверки могут проводиться внутренними силами. Для проведения проверок могут использоваться сторонние организации.

Проверка должна включать в себя следующие этапы:

а) проверка соответствия области применения поставленным задачам;

б) проверка всех важных допущений для обеспечения уверенности в том, что они являются правдоподобными в условиях имеющейся информации;

в) подтверждение аналитиком правильности использованных методов, моделей и данных;

г) проверка результатов анализа на повторяемость с привлечением персонала, не участвующего в выполнении анализа;

д) проверка результатов анализа на устойчивость по отношению к различным форматам данных.

При наличии соответствующей возможности рекомендуется сопоставлять результаты анализа с наблюдениями.

4.6 Документальное обоснование

Отчет об анализе риска документально обосновывает процесс анализа риска и должен включать в себя либо план анализа риска, либо ссылки на него и результаты оценки опасности. Техническая информация, представленная в отчете является важной частью процесса анализа риска. Оценки риска должны быть представлены в доступной форме. В отчете должны быть разъяснены преимущества и ограничения используемых критериев риска. Пояснения относительно неопределенностей, соответствующих риску, должны быть изложены на языке, понятном предполагаемому читателю.

Размер отчета зависит от целей и области применения анализа риска. В отчете, за исключением отчетов по очень простым видам анализа, должна быть отражена следующая информация:

а) краткое изложение анализа;

б) выводы;

в) цели и область применения анализа;

г) ограничения, допущения и обоснование предложений;

д) описание соответствующих частей системы;

е) методология анализа;

ж) результаты идентификации опасностей;

и) используемые модели, в том числе допущения и их обоснования;

к) использованные данные и их источники;

л) результаты оценки величины риска;

м) анализ чувствительности и неопределенности;

н) рассмотрение и обсуждение результатов (включая рассмотрение и обсуждение трудностей исследования);

п) ссылки и рекомендации.

4.7 Корректировка результатов анализа

Если анализ риска используется для обеспечения непрерывного процесса управления риском, его необходимо выполнять и документировать таким образом, чтобы он мог корректироваться на протяжении всего жизненного цикла системы, оборудования или деятельности. Анализ должен обновляться по мере поступления новой информации и в соответствии с потребностями процесса управления.

5 Аудит

В тех случаях, когда это необходимо, для обеспечения эффективности и строгого соблюдения требований настоящего стандарта может проводиться аудит процесса анализа риска. Аудит должен проводиться лицами, непосредственно не привлеченными к участию в выполнении конкретного анализа риска. При этом должны применяться соответствующие процессы и процедуры обеспечения качества.

6 Методы анализа риска

6.1 Общие сведения

В настоящем разделе описываются наиболее распространенные методы для проведения анализа технологических систем, которые применимы к идентификации опасности и оцениванию риска, а также критерии для их выбора.

6.2 Выбор методов

Метод анализа риска должен быть:

а) научно обоснованным и соответствовать сложности и природе исследуемой системы;

б) давать результаты в форме, обеспечивающей понимание природы риска и способов его контроля;

в) типовым и обладать свойствами, обеспечивающими возможность прослеживаемости, повторяемости и контролируемости.

Должно быть представлено обоснование по выбору метода с точки зрения его уместности и пригодности. В случае сомнений в уместности и пригодности метода необходимо провести сравнение его результатов с результатами альтернативных методов. При этом результаты вычислений должны быть сопоставимыми.

Как только принято решение о проведении анализа риска, определены цели и область приме-

нения, должен быть выбран метод или методы анализа, исходя из приемлемости факторов, указанных на рисунке 3, таких, как:

а) стадия разработки системы. На ранней стадии развития системы могут применяться менее детализированные методы. Они должны совершенствоваться по мере увеличения объема информации;

б) задачи анализа. Цели и задачи анализа должны иметь прямое отношение к используемым методам. Например в том случае, если предпринимается сопоставительное исследование различных вариантов, может оказаться приемлемым использование довольно грубых моделей последствий для частей системы, не подверженных изменениям;

в) типы анализируемой системы и опасности;

г) уровень детализации потенциальной опасности. Решение относительно глубины проведения анализа должно отражать первоначальное восприятие последствий (несмотря на то, что оно может измениться после получения предварительной оценки);

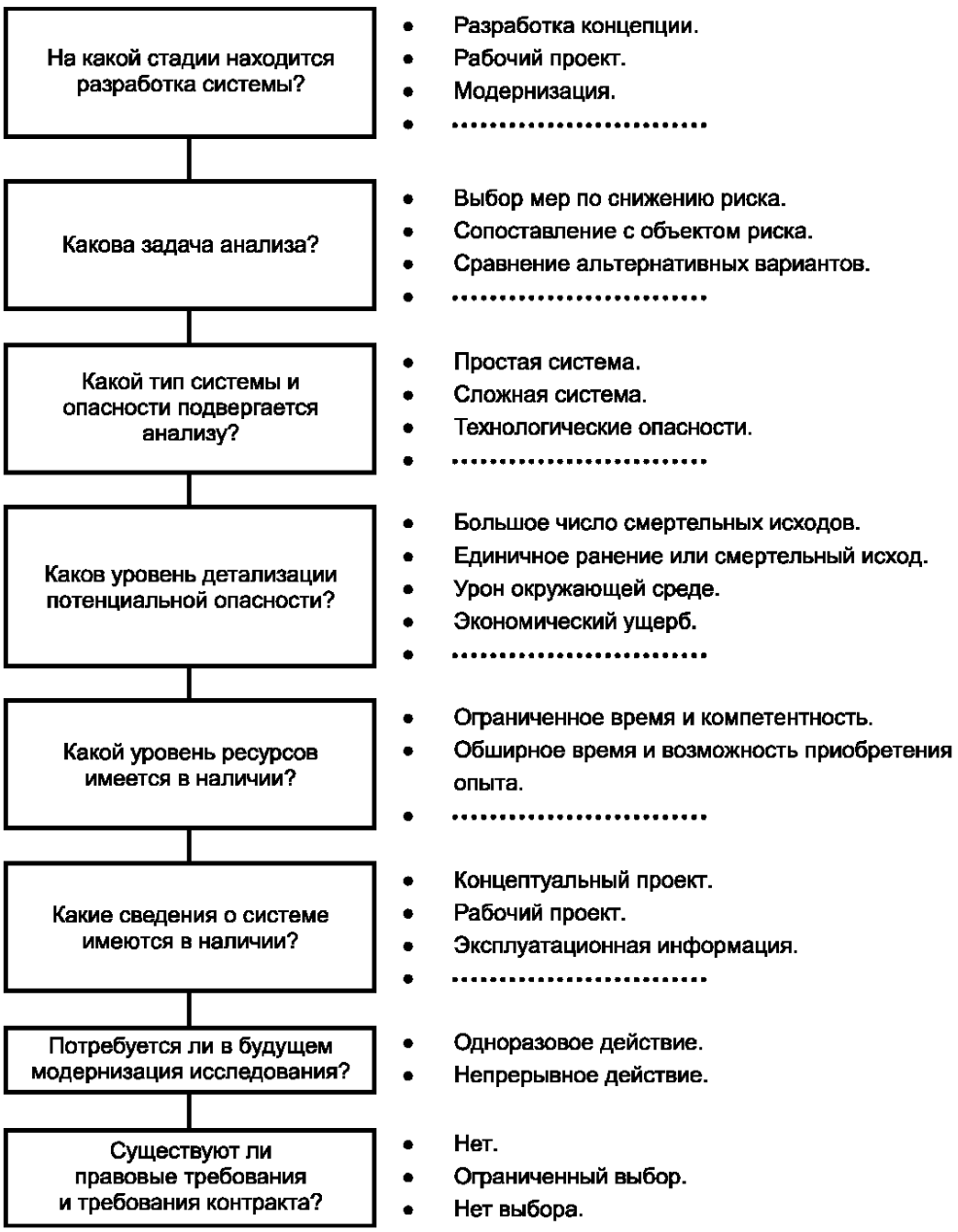


Рисунок 3 — Типовые рассуждения при выборе типа анализа и глубины исследования

д) требования к людским ресурсам, степени компетентности персонала и другим необходимым ресурсам. Простой, хорошо разработанный метод обеспечит лучшие результаты по сравнению с более усложненной процедурой, которая разработана недостаточно хорошо, поскольку он соответствует задачам и области определения анализа;

е) наличие и доступность информации и данных о системе;

ж) потребность в модификации/актуализации результатов анализа. По отношению к анализу в будущем может потребоваться его модификация/актуализация. Некоторые методы в большей степени поддаются улучшению, чем другие методы;

и) любые правовые требования и требования контракта.

6.3 Методы анализа

Перечень наиболее распространенных методов представлен в таблице 1. Перечень, приведенный в таблице 1, не является исчерпывающим. Перечень дополнительных методов представлен в таблице 2. Краткое описание некоторых методов приведено в приложении А. Иногда может оказаться необходимым использование более одного метода анализа.

6.3.1 Идентификация опасности

Идентификация опасности предполагает систематическую проверку исследуемой системы с целью идентификации типа присутствующих неустранимых опасностей и способов их проявления. Статистические записи аварий и опыт предшествующих анализов риска могут обеспечить полезный вклад в процесс идентификации опасности. Следует признать, что существует элемент субъективизма во мнениях об опасностях и что идентифицированные опасности не всегда могут быть в исчерпывающей мере теми опасностями, которые могли бы представлять угрозу для системы. Необходимо, чтобы идентифицированные опасности подвергались пересмотру при поступлении новых данных. Методы идентификации опасности в широком смысле делятся на три категории:

а) сопоставительные методы, примерами которых являются ведомости проверок, индексы опасностей и обзор данных эксплуатации;

б) фундаментальные методы, которые построены таким образом, чтобы стимулировать группу исследователей к использованию прогноза в сочетании с их знаниями по отношению к задаче идентификации опасностей путем постановки ряда вопросов типа «а что, если ... ?». Примерами данного типа методологии являются исследования опасности и связанных с ней проблем (HAZOP), а также анализ видов и последствий отказов (FMEA);

Таблица 1 — Перечень наиболее распространенных методов, используемых при анализе риска

Метод	Описание и применение	Ссылка
Анализ «дерева событий»	Совокупность приемов идентификации опасности и анализа частот, в которых используется индуктивный подход с целью перевода различных инициирующих событий в возможные исходы	А.4 приложения А
Анализ видов и последствий отказов, а также Анализ видов, последствий и критичности отказов	Совокупность приемов идентификации главных источников опасности и анализа частот, с помощью которых анализируются все аварийные состояния данной единицы оборудования на предмет их влияния как на другие компоненты, так и на систему в целом	А.2 приложения А; МЭК 60812 [1]
Анализ «дерева неисправностей»	Совокупность приемов идентификации опасности и анализа частот нежелательного события, с помощью которых определяются все пути его реализации. Используется графическое изображение	А.3 приложения А; МЭК 61025 [2]
Исследование опасности и связанных с ней проблем	Совокупность приемов идентификации фундаментальной опасности, при помощи которых оценивается каждая часть системы с целью обнаружения того, могут ли происходить отклонения от назначения конструкции и какие последствия это может повлечь	А.1 приложения А
Анализ влияния человеческого фактора	Совокупность приемов анализа частот в области воздействия людей на показатели работы системы, при помощи которых определяется влияние ошибок человека на надежность	А.6 приложения А

Окончание таблицы 1

Метод	Описание и применение	Ссылка
Предварительный анализ опасности	Совокупность приемов идентификации опасности и анализа частот, используемых на ранней стадии проектирования с целью идентификации опасностей и оценки их критичности	А.5 приложения А
Структурная схема надежности	Совокупность приемов анализа частот, на основе которых создается модель системы и ее резервов для оценки надежности системы	МЭК 61078 [3]

Таблица 2 — Перечень дополнительных методов, используемых при анализе риска

Метод	Описание и применение
Классификация групп риска по категориям	Классификация видов риска по категориям в порядке приоритетности групп риска
Ведомости проверок	Составление перечней типовых опасных веществ и/или источников потенциальных аварий, которые нуждаются в рассмотрении. С их помощью можно оценивать соответствие законам и стандартам
Общий анализ отказов	Метод, предназначенный для определения того, возможен ли случайный отказ (авария) ряда различных частей или компонентов в рамках системы, и оценки его вероятного суммарного эффекта
Модели описания последствий	Оценка воздействия события на людей, имущество или окружающую среду. Используются как упрощенные аналитические подходы, так и сложные компьютерные модели
Метод Делфи	Способ комбинирования экспертных оценок, которые могут обеспечить проведение анализа частоты, моделирования последствий и/или оценивания риска
Индексы опасности	Совокупность приемов по идентификации/оценке опасности, которые могут быть использованы для ранжирования различных вариантов системы и определения менее опасных вариантов
Метод Монте-Карло и другие методы моделирования	Совокупность приемов анализа частоты, в которых используется модель системы для оценки вариаций в исходных условиях и допущениях
Парные сопоставления	Способ оценки и ранжирования совокупности рисков путем попарного сравнения
Обзор данных по эксплуатации	Совокупность приемов, которые могут быть использованы для выявления потенциально проблемных областей, а также для анализа частоты, основанного на данных об авариях, данных о надежности и прочее
Анализ скрытых процессов	Метод выявления скрытых процессов и путей, которые могли бы привести к наступлению непредвиденных событий

в) способы индуктивного подхода, такие как логические диаграммы возможных последствий данного события (логические диаграммы «дерева событий»).

С целью усовершенствования идентификации опасности (и возможностей оценки риска) применительно к определенным проблемам могут использоваться другие приемы. Например: анализ скрытых отказов, метод Делфи и анализ влияния человеческого фактора.

Независимо от применяемых приемов важно, чтобы в общем процессе идентификации опасности должное внимание было уделено тому, что человеческие и организационные ошибки являются существенными факторами во многих авариях. Отсюда следует, что сценарии аварий, предусматривающие человеческую и организационную ошибку, также должны быть включены в процесс идентификации опасности, который не должен быть направлен исключительно на технические аспекты.

6.3.2 Оценивание риска

На практике идентификация опасности, исходящей от конкретной системы, оборудования или деятельности, может давать в качестве результата очень большое число сценариев потенциальных аварий. Детализированный количественный анализ частот и последствий не всегда осуществим. В таких ситуациях может оказаться целесообразным качественное ранжирование сценариев, помещение их в матрицы риска, указывающие различные уровни риска. Количественное определение концентрируется в таком случае на сценариях, дающих более высокие уровни риска.

На рисунке 4 представлен пример матрицы риска. Применение матрицы риска могло бы иметь своим результатом сценарии, считающиеся источником низких или незначительных рисков, снижающихся при более глубоком рассмотрении, поскольку в собирательном значении они не могли бы стать источником значительного уровня риска.

Качественная характеристика частоты события	Частота события в год	Серьезность последствия			
		Катастрофическое	Значительное	Серьезное	Незначительное
Частое	> 1	В	В	В	С
Вероятное	$1 — 10^{-1}$	В	В	С	М
Случайное	$10^{-1} — 10^{-2}$	В	В	М	М
Маловероятное	$10^{-2} — 10^{-4}$	В	В	М	М
Неправдоподобное	$10^{-4} — 10^{-6}$	В	С	Н	Н
Невероятное	$< 10^{-6}$	С	С		Н

В матрице использована следующая классификация риска:

В — высокая величина риска;

С — средняя величина риска;

М — малая величина риска;

Н — незначимая величина риска.

Применительно к данному примеру серьезность последствия определяется следующим образом:

Катастрофическое — практически полная потеря промышленного объекта или системы. Много смертельных исходов;

Значительное — крупный ущерб промышленному объекту или системе. Несколько смертельных исходов;

Серьезное — тяжелое ранение, серьезное профессиональное заболевание, серьезный ущерб промышленному объекту или системе;

Незначительное — легкое ранение, профессиональное заболевание легкой формы или незначительное повреждение системы.

Примечание — Матрица риска приведена только в качестве примера.

Рисунок 4 — Матрица риска

Имеется много матриц риска, но наиболее подходящая для конкретного анализа матрица зависит от особенностей конкретного случая. Форма используемой матрицы должна фиксироваться в отчете вместе с оцениваемыми позициями всех рассматриваемых сценариев аварий независимо от того, подвергаются ли они в дальнейшем подробному количественному анализу.

Количественный анализ риска, как правило, требует оценок как частоты (или вероятности) нежелательного события, так и ассоциирующегося с ним последствия с целью установления меры риска. Тем не менее, в некоторых случаях, когда расчеты показывают, что последствия должны быть незначительными или частота должна быть чрезвычайно низкой, может быть достаточно оценки единственного параметра.

6.3.2.1 Анализ частот

Целью анализа частот является определение частоты каждого из нежелательных событий или сценариев аварий, идентифицированных на стадии идентификации опасности. Обычно используются три основных подхода:

а) использование соответствующих данных эксплуатации с целью определения частоты, с которой данные события происходили в прошлом, и, исходя из этого, определение оценок частоты, с которой они произойдут в будущем. Используемые данные должны соответствовать типу системы, оборудования или деятельности, подлежащих рассмотрению;

б) прогнозирование частот событий с использованием таких технических приемов, как анализ диаграммы всех возможных последствий несрабатывания или аварии системы («дерева неисправностей») и анализ диаграммы возможных последствий данного события («дерева событий»). В том случае, когда статистические данные недоступны или не соответствуют требованиям, необходимо получить частоты событий посредством анализа системы и ее аварийных состояний. Числовые данные для соответствующих событий, в том числе данные о неисправности оборудования и ошибке человека, взятые из опыта эксплуатации или опубликованных данных, используются для определения оценки частоты нежелательных событий. При использовании методов прогнозирования важно обеспечить уверенность в том, что при анализе была учтена возможность нарушений режима работы системы, а также ее частей или компонентов, которые должны функционировать в случае возникновения отказов системы. При проведении анализа частот могут использоваться методы имитационного моделирования отказов оборудования и разрушений конструкции вследствие старения, а также других деградационных процессов;

в) использование мнения экспертов. Существует ряд методов для составления экспертного мнения, которые исключают двусмысленность оценок, помогают в постановке соответствующих вопросов. Экспертные оценки должны учитывать всю имеющуюся информацию, в том числе статистическую, экспериментальную, конструктивную и т. д. Имеющиеся в наличии методы предусматривают метод Делфи, парных сопоставлений, классификации групп риска и др.

Анализ диаграммы возможных отказов или аварии системы («дерева неисправностей») и анализ диаграммы возможных последствий отказов («дерева событий») изложены в приложении А. В МЭК 61025 [2] детально рассматривается анализ «дерева неисправностей».

6.3.2.2 Анализ последствий

Анализ последствий предусматривает определение результатов воздействия на людей, имущество или окружающую среду в случае наступления нежелательного события. Для расчетов рисков, касающихся безопасности (работающих или неработающих людей), анализ последствий представляет собой приблизительное определение количества людей, которые могут быть убиты, ранены или иметь серьезные поражения в том случае, если произойдет нежелательное событие.

Нежелательные события обычно состоят из таких ситуаций, как выброс токсичных материалов, пожары, взрывы, излучение частиц из разрушающегося оборудования и т. д. Модели последствий требуются для прогнозирования размера аварий, катастроф и других явлений. Знание механизма высвобождения энергии или материала и происходящих с ними последующих процессов дает возможность прогнозировать соответствующие физические процессы заранее.

Существует множество методов оценки такого рода явлений, диапазон которых простирается от упрощенных аналитических подходов до очень сложных компьютерных моделей. При использовании методов моделирования необходимо обеспечить соответствие той проблеме, которая подлежит рассмотрению.

ПРИЛОЖЕНИЕ А
(справочное)

Методы проведения анализа

А.1 Исследование опасности и связанных с ней проблем (HAZOP)

HAZOP является формой анализа видов и последствий отказов (FMEA). Исследования HAZOP первоначально были разработаны для химической промышленности. Это процедура идентификации возможных опасностей по всему объекту в целом. Она особенно полезна при идентификации непредвиденных опасностей, заложенных в объекте вследствие недостатка информации при разработке, или опасностей, проявляющихся в существующих объектах из-за отклонений в процессе их функционирования.

Основными задачами метода являются:

а) составление полного описания объекта или процесса, включая предполагаемые состояния конструкции;

б) систематическая проверка каждой части объекта или процесса с целью обнаружения путей возникновения отклонений от проектного замысла;

в) принятие решения о возможности возникновения опасностей или проблем, связанных с данными отклонениями.

Принципы исследований HAZOP могут применяться по отношению к техническим объектам в процессе их функционирования либо на различных стадиях проектирования. Исследование HAZOP, осуществляемое во время начальной стадии проектирования, может выполнять руководитель проекта.

Наиболее распространенная форма исследования HAZOP осуществляется на стадии рабочего проекта и носит название исследования HAZOP II.

Исследование HAZOP II предусматривает следующие этапы:

Этап 1 — определение целей, задач и области применения исследования, например выделение опасности, характеризующейся только нелокальными последствиями или только локальными последствиями, участков промышленного объекта, подлежащих рассмотрению, и т. д.;

Этап 2 — комплектование группы по исследованию HAZOP. Данная группа должна состоять из проектировщиков и эксплуатационников, обладающих достаточной компетентностью для оценки последствий отклонений от условий функционирования системы;

Этап 3 — сбор необходимой документации, чертежей и описаний технологического процесса. Сюда входят графики последовательности технологических операций; чертежи трубопроводов и измерительного оборудования; технические условия на оборудование, трубопроводы и измерительную аппаратуру; логические диаграммы управления технологическим процессом; проектные схемы; методики эксплуатации и технического обслуживания; методики реагирования на чрезвычайные ситуации и т. д.;

Этап 4 — анализ каждой основной единицы оборудования и всего вспомогательного оборудования, трубопроводов и контрольно-измерительной аппаратуры с использованием документов, собранных на этапе 3. В первую очередь определяется цель проектирования технологического процесса, затем применительно к каждой линии и единице оборудования по отношению к таким переменным процесса, как температура, давление, расход, уровень и химический состав, применяются слова-указатели (по таблице А.1). (Данные слова-указатели стимулируют индивидуальное мышление и побуждают к коллективному обсуждению);

Этап 5 — документальное подтверждение любого отклонения от нормы и соответствующих состояний. Кроме того, осуществляется выявление способов обнаружения и/или предупреждения отклонения. Данное документальное подтверждение обычно указывается на рабочих листах HAZOP. Образец такого рабочего листа слов-указателей «не, нет» по отношению к «расходу» представлен в таблице А.2.

Таблица А.1 — Слова-указатели HAZOP II

Слово-указатель	Определение
Нет или не	Ни одна из частей предполагаемого результата не достигается (например, нет расхода)
Больше	Количественное увеличение (например, высокое давление)
Меньше	Количественное уменьшение (например, низкое давление)
А также	Качественное увеличение (например, дополнительный материал)

Окончание таблицы А.1

Слово-указатель	Определение
Часть (чего-то)	Качественное уменьшение (например, только один или два компонента в смеси)
Обратное	Противоположное (например, противоток)
Иначе	Ни одна из частей замысла не осуществляется, происходит что-то совершенно другое (например, поток несоответствующего материала)

Таблица А.2 — Образец рабочего листа слов-указателей «не, нет» HAZOP II

Слово-указатель	Отклонение	Возможные причины	Последствия	Необходимое действие
Не, нет	Нет расхода	1) Отсутствие подаваемого материала	Выработка формуемого полимера будет снижена	а) Обеспечить хорошую связь с оператором б) Предусмотреть сигнал низкого уровня на установочном резервуаре
		2) Неисправен насос (множество причин)	Выработка формуемого полимера будет снижена	Предусмотреть сигнал низкого уровня на установочном резервуаре
		3) Закупоривание линии или ошибочно закрытый клапан или не закрывается регулирующий клапан	Насос будет перегреваться	Установить линию рециркуляции на каждом насосе

Исследование HAZOP может выделить отклонения, для которых необходима разработка смягчающих мер. В тех случаях, когда смягчающие меры неочевидны или очень дороги, результаты исследования HAZOP дают возможность идентифицировать инициирующие события, необходимые для дальнейшего анализа риска.

А.2 Анализ видов и последствий отказов (FMEA)

FMEA представляет собой метод, преимущественно качественный, хотя его можно представить и в количественной форме, при помощи которого систематически идентифицируются последствия каждого отдельного компонента аварийных состояний. Это индуктивный метод, который основан на вопросе «что случится, если ... ?». Непременной отличительной чертой в любом FMEA является рассмотрение каждого основного компонента/части системы на предмет того, каким образом он достигает аварийного состояния и как это влияет на аварийное состояние системы. Как правило, анализ является описательным и организуется в форме составления таблицы или рабочего листа, предназначенной для информации. FMEA, безусловно, относится к аварийным состояниям компонента системы, причинным факторам и воздействиям этого состояния на систему в целом и представляет их в удобной форме.

FMEA представляет собой подход по принципу «снизу вверх» и рассматривает последствия аварийных состояний компонента по принципу «одно за один раз». Этот метод способен переработать достаточное количество данных, прежде чем стать затруднительным для реализации. Кроме того, результаты могут быть легко перепроверены другим человеком, знакомым с системой.

Главными недостатками метода являются избыточность, исключение из рассмотрения восстановительно-ремонтных действий и сосредоточение на авариях единственного компонента.

FMEA может распространяться на выполнение того, что называется «Анализом видов отказов, функционирования и критичности (FMECA)». При FMECA каждый выявленный отказ ранжируется в соответствии с вероятностью его возникновения и серьезностью его последствий.

FMEA и FMECA обеспечивают вклад в анализ такого рода, как анализ «дерева неисправностей» (анализ диаграммы всех возможных последствий несрабатывания или аварии системы). Наряду с применением по отношению к компонентам системы FMEA и FMECA могут использоваться и по отношению к ошибке человека; они могут использоваться как для идентификации опасности, так и для оценки вероятности (если только в системе имеет место ограниченный уровень избыточности). Более подробно FMEA и FMECA представлены в МЭК 60812 [1].

А.3 Анализ диаграммы всех возможных последствий несрабатывания или аварии системы (анализ «дерева неисправностей» (FTA)

FTA представляет собой совокупность приемов качественных или количественных, при помощи которых выявляются методом дедукции, выстраиваются в логическую цепь и представляются в графической форме те условия и факторы, которые могут способствовать определенному нежелательному событию (называемому вершиной событий). Неисправностями или авариями, идентифицируемыми в «дереве», могут быть события, связанные с

повреждениями механической конструкции компонента, ошибками персонала или любыми другими событиями, которые влекут за собой нежелательное событие. Начиная с вершины событий выявляются возможные причины или аварийные состояния следующего, более низкого функционального уровня системы. Последующая поэтапная идентификация нежелательного функционирования системы в направлении последовательно снижающихся уровней системы приводит к искомому уровню системы, которым является аварийное состояние компонента. Пример «дерева неисправностей» для аварийного генератора представлен на рисунке А.1. Таблица наиболее распространенных символов «дерева неисправностей» представлена на рисунке А.2.

FTA предоставляет возможность подхода, который является в высокой степени системным, но в то же время достаточно гибким для того, чтобы обеспечить возможность анализа множества факторов, включая взаимодействия людей и физические явления. Применение подхода по принципу «сверху вниз», неявного по своей методике, концентрирует внимание на тех воздействиях неисправности или аварии, которые имеют непосредственное отношение к вершине событий. Это представляет собой определенное преимущество, несмотря на то, что может стать и причиной утраты тех воздействий, которые являются существенно важными где-нибудь еще. FTA особенно полезен для анализа систем с множеством областей контакта и взаимодействий. Графическое представление приводит к тому, что можно без особого труда понять поведение системы и поведение включенных в него факторов, но поскольку размер «деревьев» зачастую велик, обработка «деревьев неисправностей» может потребовать применения компьютерных систем. Эта отличительная черта также затрудняет проверку «дерева неисправностей».

FTA можно использовать для идентификации опасностей, хотя в первую очередь он используется при оценке риска в качестве инструмента для оценки вероятностей или частот неисправностей и аварий. Более детальные подробности, касающиеся FTA, представлены в МЭК 61025 [2].

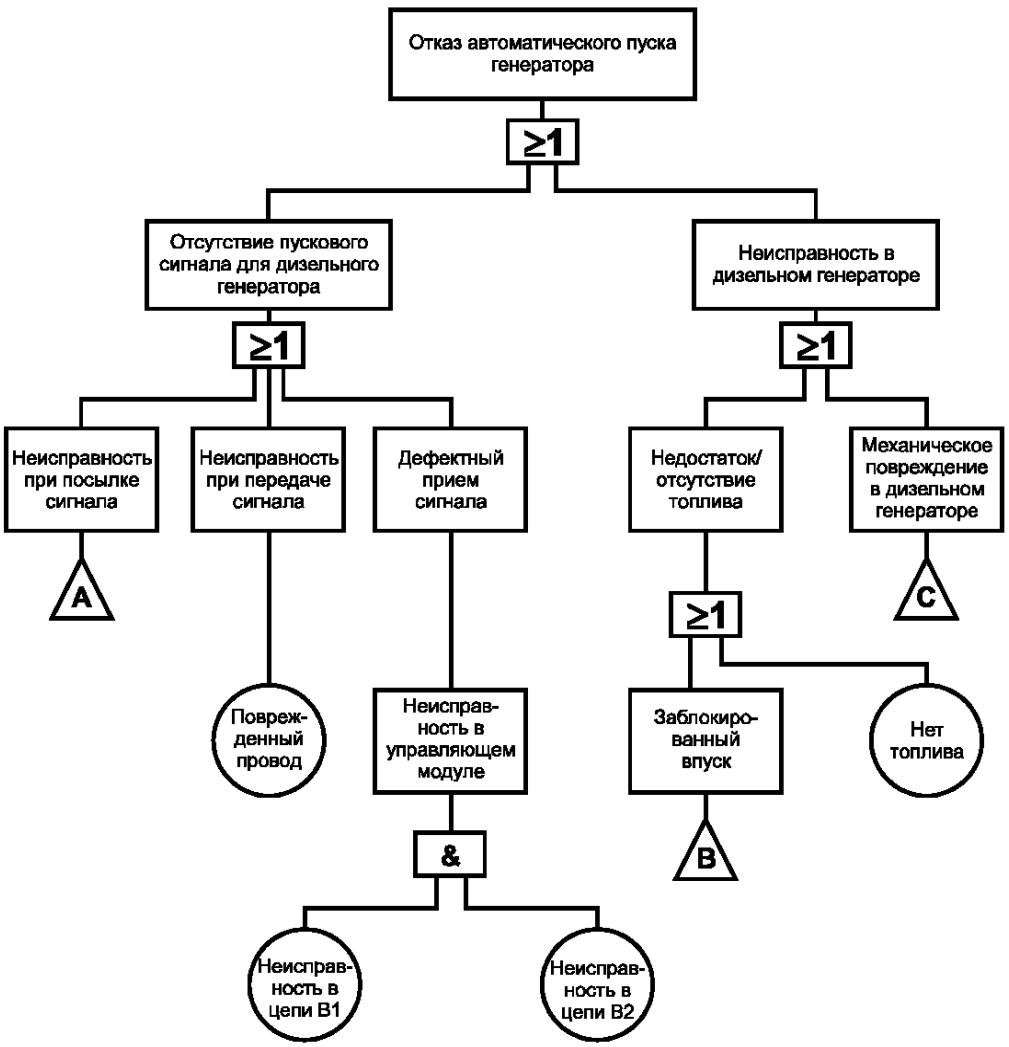
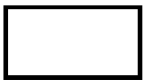
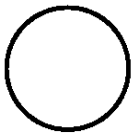


Рисунок А.1 — Пример «дерева неисправностей»

Символ	Функция	Описание
	Блок описания события	Наименование или описание события, код события и вероятность его появления (по мере необходимости) должны быть включены в рамку символа
	Базовое событие	Событие, которое не может быть подразделено
	Переключатель И	Событие происходит только в том случае, если одновременно происходят все составляющие события
	Переключатель ИЛИ	Событие происходит в том случае, если происходит любое из составляющих событий либо в единственном числе, либо в любом из сочетаний
	Вход в блок	Событие, определяемое где-нибудь в другом месте «дерева неисправностей»

Примечание — Символы взяты из МЭК 61025 [2] и использованы на рисунке А.1. (Существуют также альтернативные условные обозначения символов «дерева неисправностей»).

Рисунок А.2 — Символы «дерева неисправностей»

А.4 Анализ диаграммы возможных последствий события (анализ «дерева событий») (ETA)

ETA представляет собой совокупность приемов количественных или качественных, которые используются для идентификации возможных исходов инициирующего события и, если это требуется, их вероятностей. ETA широко используется для объектов, характеризующихся особенностями проекта, которые способствуют снижению аварийности и позволяют выявлять последовательности событий, которые, в свою очередь, приводят к появлению определенных последствий инициирующего события. Предполагается, что каждое событие в последовательности представляет собой либо исправность, либо неисправность. Простое «дерево событий» для взрыва пыли с указанными на нем вероятностями представлено на рисунке А.3. Следует отметить, что вероятности на «дереве событий» являются условными вероятностями. Например, вероятность функционирования разбрызгивателя не является вероятностью, полученной на основании испытаний при нормальных условиях, а является вероятностью функционирования в условиях пожара, вызванного взрывом.

ETA представляет собой индуктивный тип анализа, в котором основным задаваемым вопросом является «что случится, если ... ?». Он обеспечивает взаимосвязь между функционированием (или отказом) разнообразных смягчающих систем и опасным событием, следующим после того, как происходит единичное инициирующее событие. ETA очень полезен при выявлении событий, которые требуют дальнейшего анализа с использованием FTA (то есть вершины событий «деревьев неисправностей»). Для того, чтобы иметь возможность сделать исчерпывающую оценку риска, требуется идентифицировать все потенциальные инициирующие события. При данном методе, тем не менее, всегда существует вероятность упустить из виду некоторые важные инициирующие события. Более того, в случае «деревьев событий» мы имеем дело только с состояниями успеха и отказа. Возникает трудность с включением запаздывающего успеха или возвратных событий.

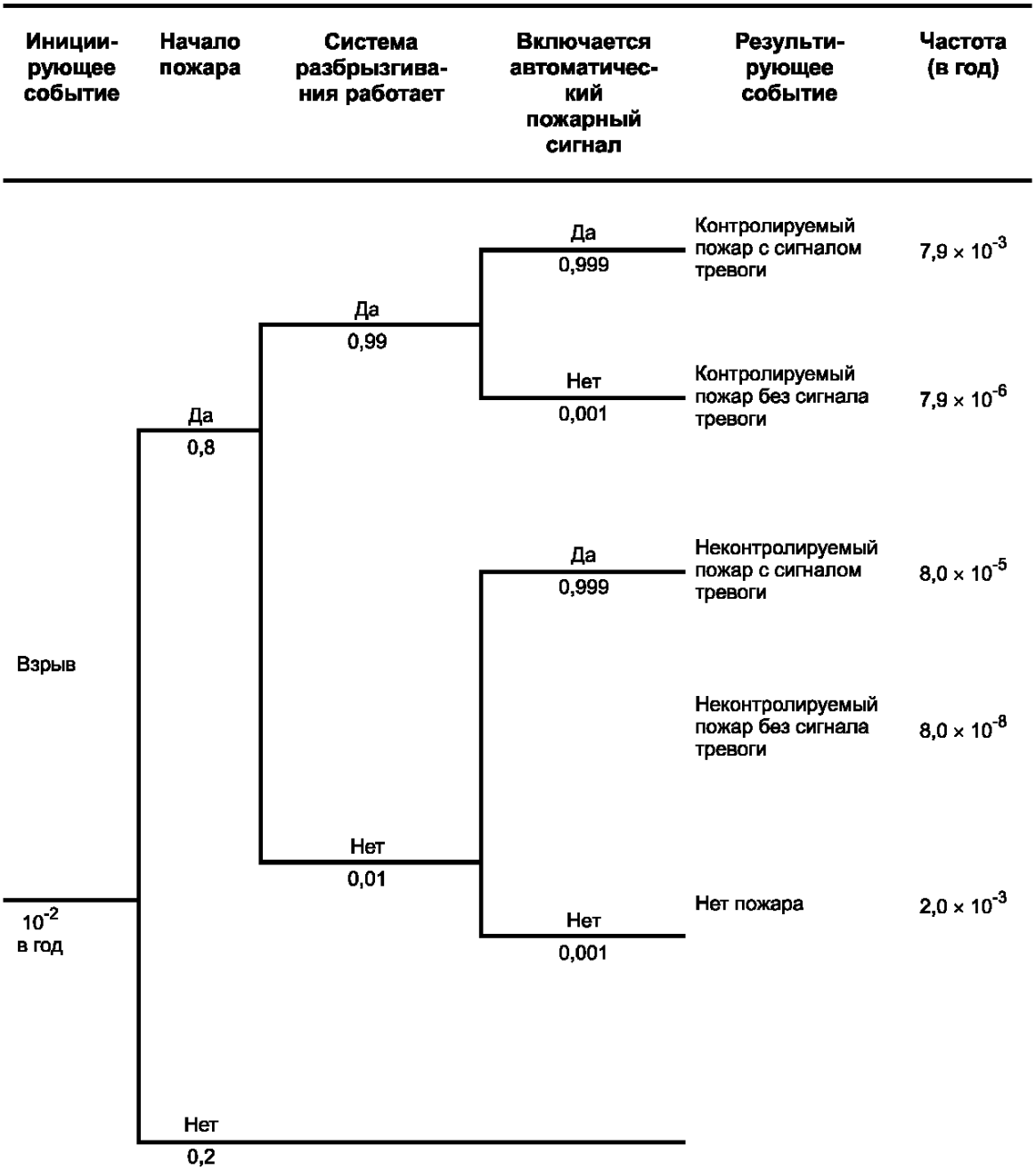


Рисунок А.3 — Пример «дерева событий» для взрыва пыли

ETA может быть использован как для идентификации опасности, так и для вероятностной оценки последовательности событий, влекущих за собой опасные ситуации.

А.5 Предварительный анализ опасности (PHA)

PHA представляет собой индуктивный метод анализа, задачей которого является идентификация опасностей, опасных ситуаций и событий, которые могут причинить вред данной деятельности, объекту или системе. Чаще всего его принято проводить на ранней стадии разработки проекта, когда мало информации по деталям конструкции и рабочим процедурам, и зачастую он может быть предшественником последующих исследований. Кроме того, он может оказаться полезным в тех случаях, когда анализируются существующие системы или устанавливаются приоритеты опасностей, где обстоятельства препятствуют использованию более обширной совокупности технических приемов.

При проведении PHA вырабатывается перечень опасностей и опасных ситуаций общего характера посредством рассмотрения таких характеристик, как:

а) используемые или производимые материалы и их способность вступать в реакцию;
б) применяемое оборудование;
в) условия окружающей среды;
г) схема расположения;
е) области контакта и взаимодействия между компонентами системы и т. д.

Реализация данного метода завершается определением возможностей аварии, качественной оценкой величины возможного вреда или ущерба здоровью, который мог быть нанесен, и идентификацией возможных исправительных мер. РНА должен корректироваться на стадиях проектирования, изготовления и испытания для обнаружения новых опасностей, внесения поправок и его совершенствования. Полученные результаты могут быть представлены различными способами, например в виде таблиц и «деревьев».

А.6 Оценка влияния на надежность человеческого фактора (HRA)

А.6.1 Общие положения

Оценка связана с влиянием человеческого фактора, а именно операторов и обслуживающего персонала, на работу системы и может быть использована для оценки воздействия ошибок персонала на безопасность и производительность.

Многие процессы содержат потенциальные возможности для ошибок персонала, в особенности в тех случаях, когда время, которым располагает оператор для принятия решений, ограничено. Вероятность того, что проблемы будут развиваться негативным образом, зачастую мала. Иногда действия со стороны персонала ограничиваются возможностью предотвращения начальной неисправности, прогрессирующей в направлении аварии.

При помощи HRA идентифицируются разнообразные типы ошибочных действий, которые могут иметь место, в том числе следующие:

а) ошибка по оплошности, недосмотр, выразившийся в невыполнении требуемого действия;
б) ошибка несоответствия, которая может предусматривать:
1) положение, когда требуемое действие выполняется несоответствующим образом;
2) действие, выполняемое слишком большим или слишком малым усилием либо без требуемой точности;
3) действие, выполняемое в неподходящее для него время;
4) действие (или действия), выполняемое в неправильной очередности;
в) лишнее действие, ненужное действие, выполняемое вместо требуемого действия или в дополнение к нему.

В результате HRA выявляются действия, которые могут воссоздать предшествующие ошибки.

Методология HRA является смешанной дисциплиной, в которой заняты исследователи и практики, являющиеся, как правило, специалистами в сферах либо теории и практики надежности, либо психологии и человеческих факторов.

Важность HRA была проиллюстрирована различными авариями, в которых критические ошибки человека способствовали катастрофической последовательности событий. Такого рода аварии являются предостережением от оценок риска, которые концентрируют внимание исключительно на механической конструкции и программных средствах в системе. Они иллюстрируют опасность игнорирования ошибок персонала. Более того, HRA являются полезными при рассмотрении ошибок, снижающих производительность, и при выявлении тех путей, которыми эти ошибки и другие неисправности (механической конструкции и программного обеспечения) могут быть «воспроизведены» людьми, операторами и обслуживающим персоналом.

HRA может включать в себя следующие этапы:

1) анализ задачи;
2) выявление ошибки персонала;
3) количественное определение влияния на надежность человеческого фактора.

Анализ задачи и выявление ошибки персонала необходимо начинать на стадии концепции и на ранних этапах проектирования и разработки. Они должны модернизироваться на более поздних стадиях развития системы.

А.6.2 Анализ задачи (TA)

Целью ТА в процессе HRA является подробное описание и определение характера задачи, подлежащей анализу, для выявления ошибки персонала и/или количественной оценки влияния на надежность человека. Анализ задачи может также проводиться для других целей, таких как оценка взаимодействия человека с машиной или планирование процедуры.

А.6.3 Выявление ошибки персонала (HEI)

На данном этапе идентифицируются и описываются возможные ошибочные действия при исполнении задачи. Выявление ошибки персонала может включать выявление возможных последствий и причин ошибочных действий, а также предложение мер по снижению вероятности этой ошибки, совершенствованию перспектив для исправления и/или уменьшению последствий ошибочных действий. Результаты HEI, таким образом, обеспечивают ценный вклад в управление риском даже в том случае, если не проводится никакая количественная оценка.

А.6.4 Количественная оценка влияния на надежность человеческого фактора (HRQ)

Целью HRQ является оценка вероятности правильного выполнения задачи или вероятности ошибочных действий. Некоторые технические приемы могут также предусматривать шаги по оценке вероятности или частоты определенных последовательностей нежелательных событий или нежелательных исходов.

ПРИЛОЖЕНИЕ Б
(справочное)

Библиография*

[1] МЭК 60812: 1985 Техника анализа надежности систем. Метод анализа вида и последствий отказов (FMEA)
[2] МЭК 61025: 1990 Анализ диагностического дерева отказов (FTA)
[3] МЭК 61078: 1991 Методика анализа надежности. Метод блок-системы надежности

* Оригиналы международных стандартов МЭК — во ВНИИКИ Госстандарта России.

УДК 362:621.001:658.382.3:006.354 ОКС 13.110 Т58 ОКСТУ 0012

Ключевые слова: риск, опасность, оценка риска, оценка величины риска, идентификация опасности, оценивание риска, ущерб, анализ риска, виды и последствия отказов, дерево неисправностей, анализ опасности

Редактор *Т.С. Шеко*
Технический редактор *Л.А. Гусева*
Корректор *Н.Л. Рыбалко*
Компьютерная верстка *А.Н. Золотаревой*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 08.08.2002. Подписано в печать 21.10.2002. Усл.печ.л. 3,26. Уч.-изд.л. 2,70.
Тираж 800 экз. С 7805. Зак. 913.

ИПК Издательство стандартов, 107076 Москва, Колодезный пер., 14.
http: //www.standards.ru e-mail: info@standards.ru
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", 103062 Москва, Лялин пер., 6.
Плр № 080102