ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61511-3— 2011

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ. СИСТЕМЫ БЕЗОПАСНОСТИ ПРИБОРНЫЕ ДЛЯ ПРОМЫШЛЕННЫХ ПРОЦЕССОВ

Часть 3

Руководство по определению требуемых уровней полноты безопасности

IEC 61511-3:2003
Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidelines for the determination of the required safety integrity levels (IDT)

Издание официальное

Москва
Стандартинформ
2012

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2011 г. № 470-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61511-3:2003 «Безопасность функциональная. Системы безопасности, приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности» (IEC 61511-3:2003 «Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidelines for the determination of the required safety integrity levels»).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

Содержание

Введение

Приборные системы безопасности уже в течение многих лет используются для выполнения функций безопасности в промышленных процессах. Для эффективного применения приборных систем безопасности при выполнении функций безопасности необходимо, чтобы они соответствовали определенному минимальному уровню стандартизации.

Область применения настоящего стандарта — приборные системы безопасности, применяемые в промышленных процессах. Он также устанавливает необходимость проведения оценки опасности и риска процесса для обеспечения формирования спецификации приборных систем безопасности. Вклад других систем безопасности может быть учтен только при рассмотрении требований к эффективности приборных систем безопасности. Приборная система безопасности включает все компоненты и подсистемы, необходимые для выполнения функции безопасности, от датчика(ов) до исполнительного(ых) элемента(ов).

В основе настоящего стандарта лежат две фундаментальные концепции, необходимые для его применения: концепция жизненного цикла безопасности и концепция уровней полноты безопасности.

Настоящий стандарт рассматривает приборные системы безопасности, использующие электрические/электронные/программируемые электронные технологии. Если для логических устройств используют другие принципы действия, то следует применять основные положения настоящего стандарта. Настоящий стандарт также рассматривает датчики и исполнительные элементы приборной системы безопасности независимо от принципа их действия. Настоящий стандарт является конкретизацией общего подхода к вопросам обеспечения безопасности, представленного в МЭК 61508, для промышленных процессов (см. МЭК 61511-1, приложение А).

Настоящий стандарт устанавливает подход, минимизирующий стандартизацию деятельности для всех стадий жизненного цикла безопасности. Этот подход был принят в целях реализации рациональной и последовательной технической политики.

В большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. При необходимости он может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск. Системы защиты основаны на применении различных технологий: химических, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных. Любая стратегия обеспечения безопасности должна рассматривать каждую конкретную приборную систему безопасности в контексте других систем защиты. Для облегчения применения такого подхода настоящий стандарт:

- требует, чтобы выполнялась оценка опасностей и рисков для определения общих требований к безопасности;
- требует, чтобы выполнялось распределение требований к безопасности в (по) приборной(ым) системе(ам) безопасности;
- реализует подход, который применим ко всем приборным методам обеспечения функциональной безопасности;
- подробно рассматривает применение определенных действий, таких как руководство работами по безопасности, которые могут быть применены ко всем методам обеспечения функциональной безопасности.

Настоящий стандарт по приборным системам безопасности для промышленных процессов:

- охватывает все стадии жизненного цикла безопасности — от разработки первоначальной концепции, проектирования, внедрения, эксплуатации и технического обслуживания вплоть до утилизации;
- дает возможность, чтобы существующие или новые стандарты в разных странах, регламентирующие конкретные промышленные процессы, были с ним гармонизированы.

Настоящий стандарт призван привести к высокому уровню согласованности (например, основных принципов, терминологии, информации) в рамках конкретных промышленных процессов. Это принесет преимущества как в плане безопасности, так и в плане экономики.

В пределах своей юрисдикции соответствующие регулирующие органы (например, национальные, федеральные, штата, провинции, округа, города) могут устанавливать требования к проектированию безопасности процесса, к управлению безопасностью процесса или другие требования, которые должны превалировать над требованиями, определенными в настоящем стандарте.

Настоящий стандарт содержит руководство по определению требуемых уровней полноты безопасности, используя анализ опасности и риска (АОР). Содержащаяся в настоящем стандарте информация предназначена для проведения глубокого анализа различных общих методов применения АОР. Для применения любого из этих методов представленной информации недостаточно.

Перед применением настоящего стандарта следует ознакомиться с концепцией и определением понятия «уровень полноты безопасности», приведенными в МЭК 61511-1. Приложения к настоящему стандарту рассматривают следующие вопросы:

Приложение A содержит обзор основных положений метода приемлемого риска и метода ALARP.

Приложение B содержит обзор полуколичественного метода определения требуемого УПБ.

Приложение C содержит обзор метода матриц безопасности для определения требуемого УПБ.

Приложение D содержит обзор метода, использующего для определения требуемого УПБ полукачественный подход графа рисков.

Приложение E содержит обзор метода, использующего для определения требуемого УПБ качественный подход графа рисков.

Приложение F содержит обзор метода, использующего для выбора требуемого УПБ анализ слоев защиты (АСЗ).

На рисунке 1 представлена общая структура настоящего стандарта.

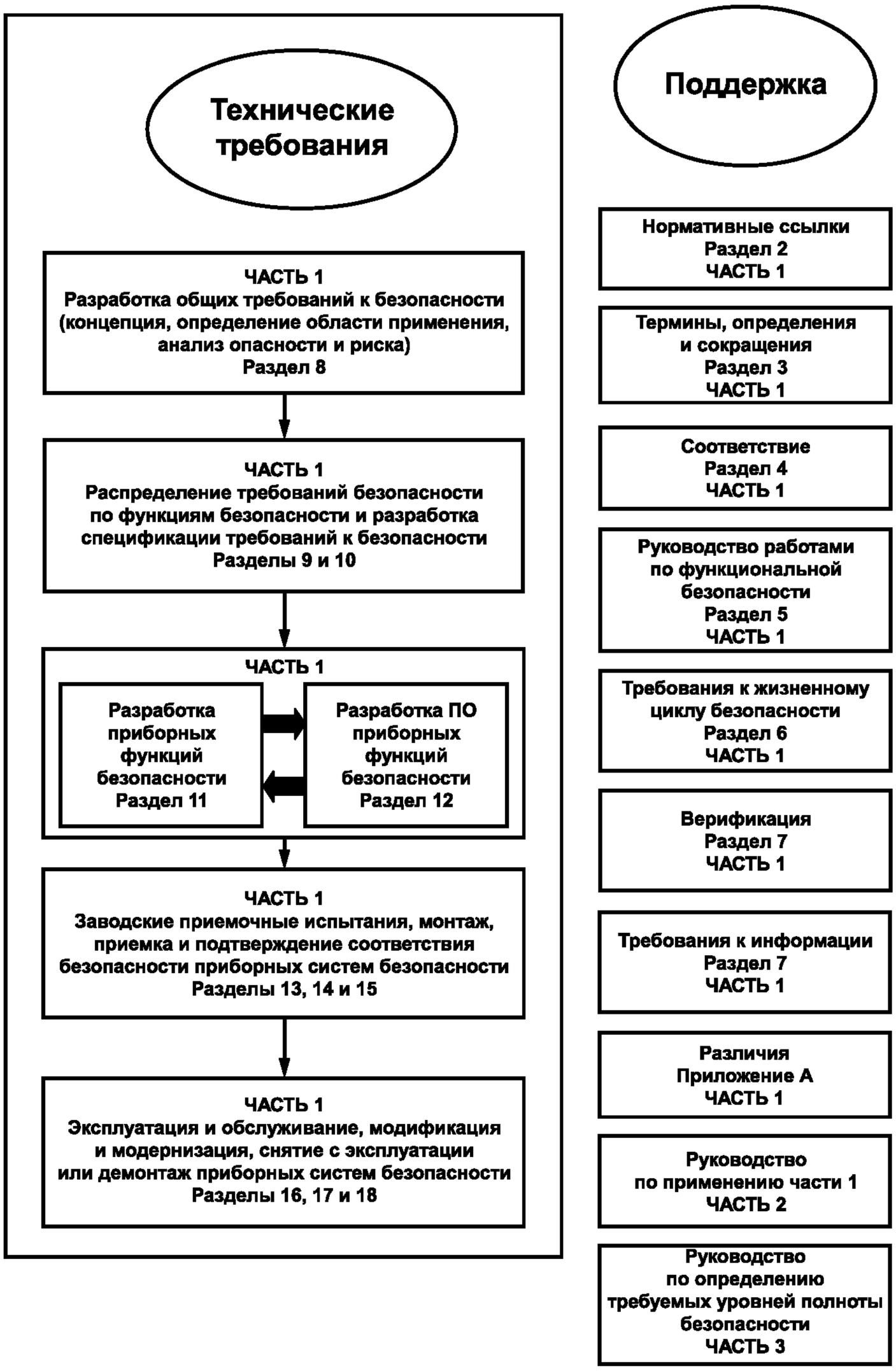


Рисунок 1 — Общая структура настоящего стандарта

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ. СИСТЕМЫ БЕЗОПАСНОСТИ ПРИБОРНЫЕ ДЛЯ ПРОМЫШЛЕННЫХ ПРОЦЕССОВ

Часть 3

Руководство по определению требуемых уровней полноты безопасности

Functional safety. Safety instrumented systems for the process industry sector.
Part 3. Guidelines for the determination of the required safety integrity levels

Дата введения — 2012—08—01

1 Область применения

Настоящий стандарт содержит:

- основные положения концепции риска и описание отношения между риском и полнотой безопасности (см. раздел 3);
- определение допустимого риска (см. приложение А);
- описание различных методов, позволяющих определить уровень полноты безопасности (УПБ) для функций безопасности приборных систем безопасности (ПСБ) (см. приложения B, C, D, E и F).

В частности, настоящий стандарт:

a) применяют в случаях, когда функциональная безопасность достигается путем использования одной или более функций безопасности ПСБ для защиты персонала, населения или окружающей среды;

b) может быть применен на объектах, не требующих обеспечения безопасности, например для защиты имущества;

c) иллюстрирует типичные методы оценки опасностей и рисков, которые могут быть проведены для определения требований к функциональной безопасности и к УПБ каждой из функций безопасности ПСБ;

d) иллюстрирует методы и/или средства, позволяющие определить требуемые УПБ;

e) содержит структуру работ по установлению УПБ, но не определяет УПБ для конкретных случаев применения;

f) не содержит примеров определения требований к иным методам снижения рисков.

Приложения B, C, D, E и F упрощенно иллюстрируют количественный и качественный подходы. Эти приложения были включены лишь для иллюстрации общих принципов, положенных в основу ряда используемых методов, и не могут служить руководством к их практическому применению.

Примечание — Тем, кто намеревается практически использовать методы, описанные в упомянутых приложениях, следует обратиться к ссылкам, имеющимся в каждом приложении.

На рисунке 2 показана совокупность методов снижения риска.

Издание официальное

Рисунок 2 — Типовые способы снижения риска, встречающиеся на технологических объектах (модель слоев защиты)

2 Термины, определения и сокращения

В настоящем стандарте применены термины, определения и сокращения, приведенные в МЭК 61511-1 (раздел 3).

3 Риск и полнота безопасности. Общие требования

3.1 Общие сведения

В данном разделе приведена информация об основополагающих концепциях риска и связи рисков с полнотой безопасности. Эта информация является общей для всех рассматриваемых ниже методов оценки различных опасностей и рисков.

3.2 Необходимая степень снижения риска

Необходимая степень снижения риска (которая может быть установлена либо качественно[1)], либо количественно[2)]) — это такое снижение риска, которое должно быть обеспечено для достижения уровня риска (заданного уровня безопасности процесса), приемлемого в конкретной ситуации. Концепция необходимого снижения риска является фундаментально важной для формулирования технических

[1)] При определении необходимой степени снижения риска следует предварительно установить приемлемый риск. В МЭК 61508-5 (приложения D и E) перечислены соответствующие количественные методы, хотя в рассмотренных там примерах необходимое снижение риска представлено, скорее, в неявном виде.

[2)] Например, опасное событие, приводящее к определенным последствиям, как правило, характеризуется максимальной частотой повторений в год.

требований к безопасности функций безопасности ПСБ (особенно в части требований к полноте безопасности спецификации требований к безопасности). Цель определения приемлемого риска (заданного уровня безопасности процесса) в случае конкретного опасного события состоит в установлении величины «разумного» риска, учитывающего как частоту возникновения опасных событий, так и их специфические последствия. Слои защиты (см. рисунок 3) разрабатываются так, чтобы уменьшить частоту возникновения опасных ситуаций и/или их последствия.

Важными факторами для оценки величины приемлемого риска являются восприятие и точки зрения тех лиц, которые подвергаются опасности. При определении приемлемого риска для конкретного применения необходимо учитывать:

- указания соответствующих регулирующих органов;
- обсуждения и соглашения между различными сторонами, принимающими участие в данном применении;
- промышленные стандарты и руководства;
- промышленные, экспертные и научные советы;
- законодательные и регулирующие требования, как общие, так и относящиеся к конкретному применению.

3.3 Роль приборных систем безопасности

ПСБ реализует функции безопасности, необходимые для достижения или для поддержания безопасного состояния процесса, и, следовательно, вносит вклад в решение задачи необходимого снижения риска для достижения приемлемого риска. Например, в спецификации требований к функциям безопасности может быть указано, что если температура достигает значения *x*, то клапан *y* открывается, обеспечивая поступление воды в емкость.

Необходимое снижение риска может достигаться с помощью одной или нескольких ПСБ либо с помощью других слоев защиты.

В выполнении функции безопасности может участвовать человек. Например, оператор может получать информацию о состоянии процесса и выполнять основанные на этой информации защитные действия. Если человек является частью функции безопасности, то должны быть учтены все человеческие факторы.

ПСБ может действовать по запросу или в непрерывном режиме.

3.4 Полнота безопасности

Считается, что полнота безопасности состоит из двух частей:

a) **полнота безопасности аппаратных средств** — это часть полноты безопасности, связанная со случайными отказами аппаратных средств, причем относящимися к опасным отказам. Факт достижения установленного уровня полноты безопасности аппаратных средств можно оценить с разумным уровнем точности. Поэтому требования могут быть распределены между подсистемами, используя известные правила произведения вероятностей и учитывая отказы по общей причине. Для достижения требуемой полноты безопасности аппаратных средств может оказаться необходимым применение структуры с резервированием;

b) **систематическая полнота безопасности** — эта часть полноты безопасности связана с систематическими отказами, относящимися к опасным отказам. Хотя влияние отдельных систематических отказов на полноту безопасности можно оценить, данные по отказам, вызванным ошибками при проектировании, и отказам по общей причине указывают на то, что влияние этих отказов бывает сложно предсказать. При этом увеличивается неопределенность в расчетах вероятности отказов в конкретной ситуации (например, вероятности отказов ПСБ). Следовательно, необходимо решить, какие способы минимизации этой неопределенности окажутся наиболее эффективными. Нужно отметить, что меры, принятые для уменьшения вероятности случайных отказов аппаратных средств, не должны обязательно приводить к снижению вероятности систематических отказов. Такие технические решения, как резервирование в виде организации параллельных каналов с идентичным оборудованием, которые являются весьма эффективными для случайных отказов аппаратных средств, мало полезны для уменьшения систематических отказов.

Общее снижение риска, достигаемое функциями безопасности ПСБ вместе со средствами других слоев защиты, должно быть таким, чтобы обеспечить:

- частоту отказов функций безопасности, достаточно низкую для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску, и/или

- возможность того, что функции безопасности так изменяют последствия отказов, чтобы риск не превышал значение приемлемого риска.

Рисунок 3 иллюстрирует общую концепцию снижения риска. Общая модель предполагает следующее:

- имеется процесс и связанная с ним основная система управления процессом (ОСУП);
- существует связанный с процессом человеческий фактор;
- слои защиты безопасности включают в свой состав:
  1) механическую систему защиты,
  2) приборные системы безопасности,
  3) механическую систему ослабления последствий.

Примечание — На рисунке 3 представлена обобщенная модель риска, иллюстрирующая общие принципы. Модель риска для конкретного случая должна составляться с учетом конкретных приемов, с помощью которых на базе ПСБ и других слоев защиты фактически достигается необходимое снижение риска. Результирующая модель риска в конкретном случае может отличаться от представленной на рисунке 3.

На рисунках 3 и 4 показаны следующие риски:

- риск процесса. Это риск наличия конкретного опасного события для процесса. При этом учитывается наличие основной системы управления процессом и человеческого фактора. При определении этого риска не рассматриваются какие бы то ни было специальные средства защиты безопасности;
- приемлемый риск (заданный уровень безопасности процесса). Риск, который считается приемлемым в данном контексте на основе принятой в обществе системы ценностей;
- остаточный риск. В контексте настоящего стандарта это риск возникновения опасных событий при условии применения всей совокупности слоев защиты.

Риск процесса является функцией от риска, связанного с самим процессом, но учитывающего также снижение риска, достигнутое благодаря применению системы управления процессом. Для того чтобы избежать неразумных требований к полноте безопасности ОСУП, настоящий стандарт устанавливает ограничения на возможные требования.

Необходимое снижение риска — это уменьшение уровня риска до такого минимального значения, который необходим для обеспечения приемлемого риска. Оно может достигаться с помощью как одного способа, так и комбинацией способов снижения риска. Процесс необходимого снижения риска, обеспечивающий достижение конкретного приемлемого риска от начального значения риска процесса, показан на рисунке 3.

3.5 Риск и полнота безопасности

Очень важно полностью осознать разницу между риском и полнотой безопасности. Риск — это мера частоты появления и последствий конкретного опасного события. Его можно оценить для различных ситуаций (риск процесса, приемлемый риск, остаточный риск и т. д., см. рисунок 3). При определении приемлемого риска учитывают социальные и политические факторы. Полнота безопасности — это мера вероятности того, что функция безопасности ПСБ и другие слои защиты обеспечат установленную безопасность. Только после того, как приемлемый риск установлен и получена оценка величины необходимого снижения риска, можно определить требования к полноте безопасности ПСБ.

Примечание — Такая процедура может носить итеративный характер, что позволит осуществить оптимизацию разработки в целях выполнения различных требований.

Роль, которую играют функции безопасности при достижении необходимого снижения риска, показаны на рисунках 3 и 4.

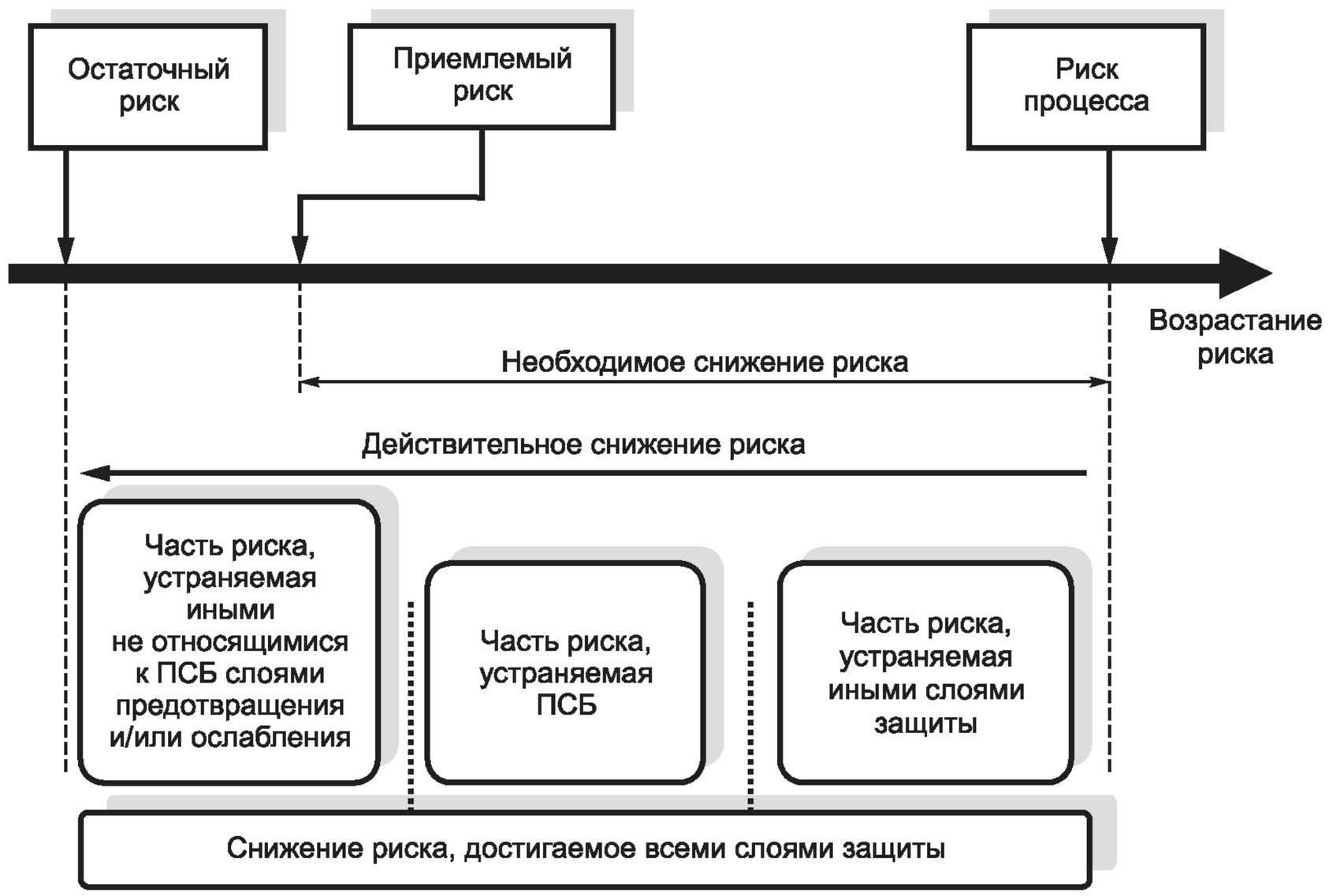


Рисунок 3 — Общая концепция снижения риска

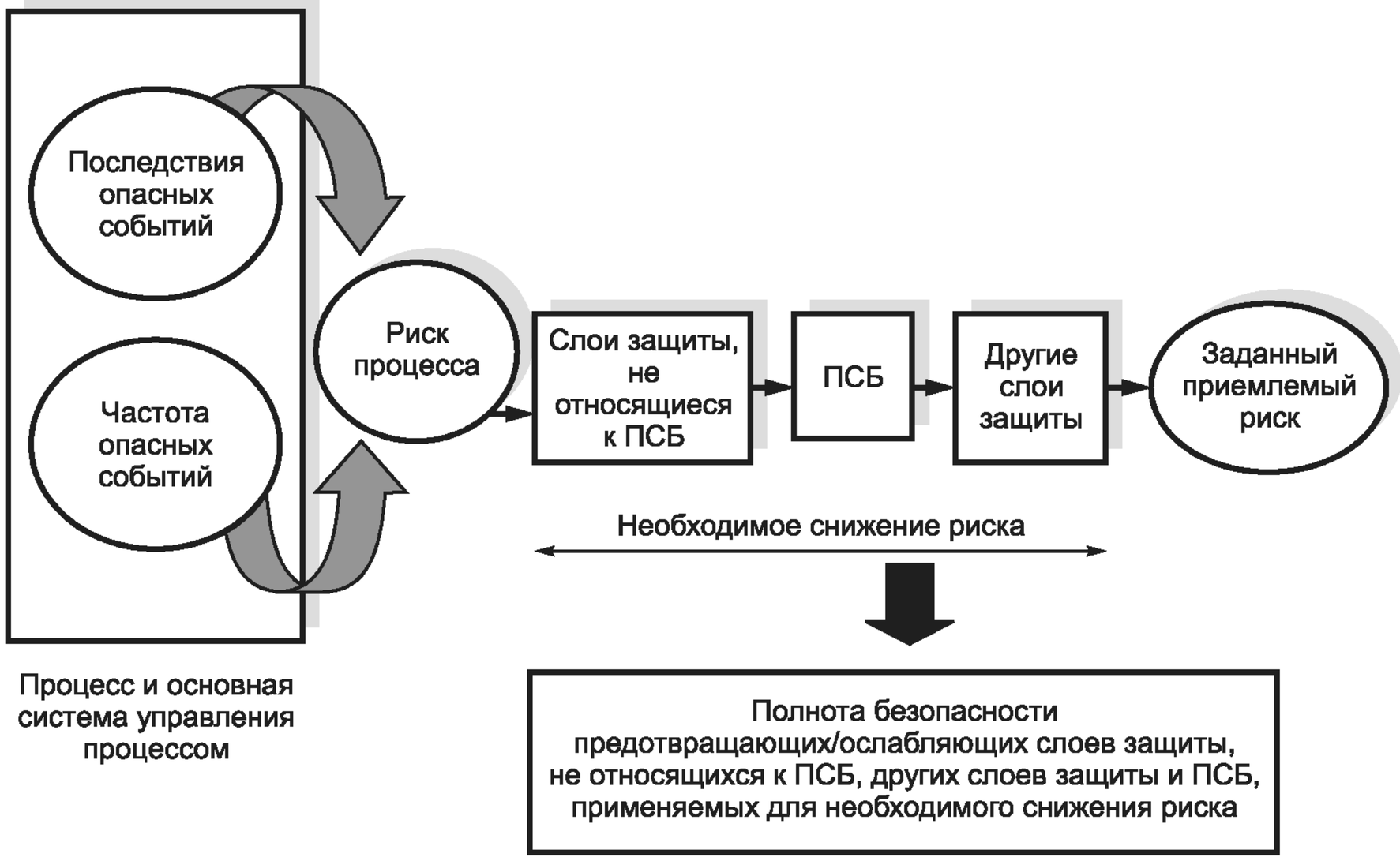
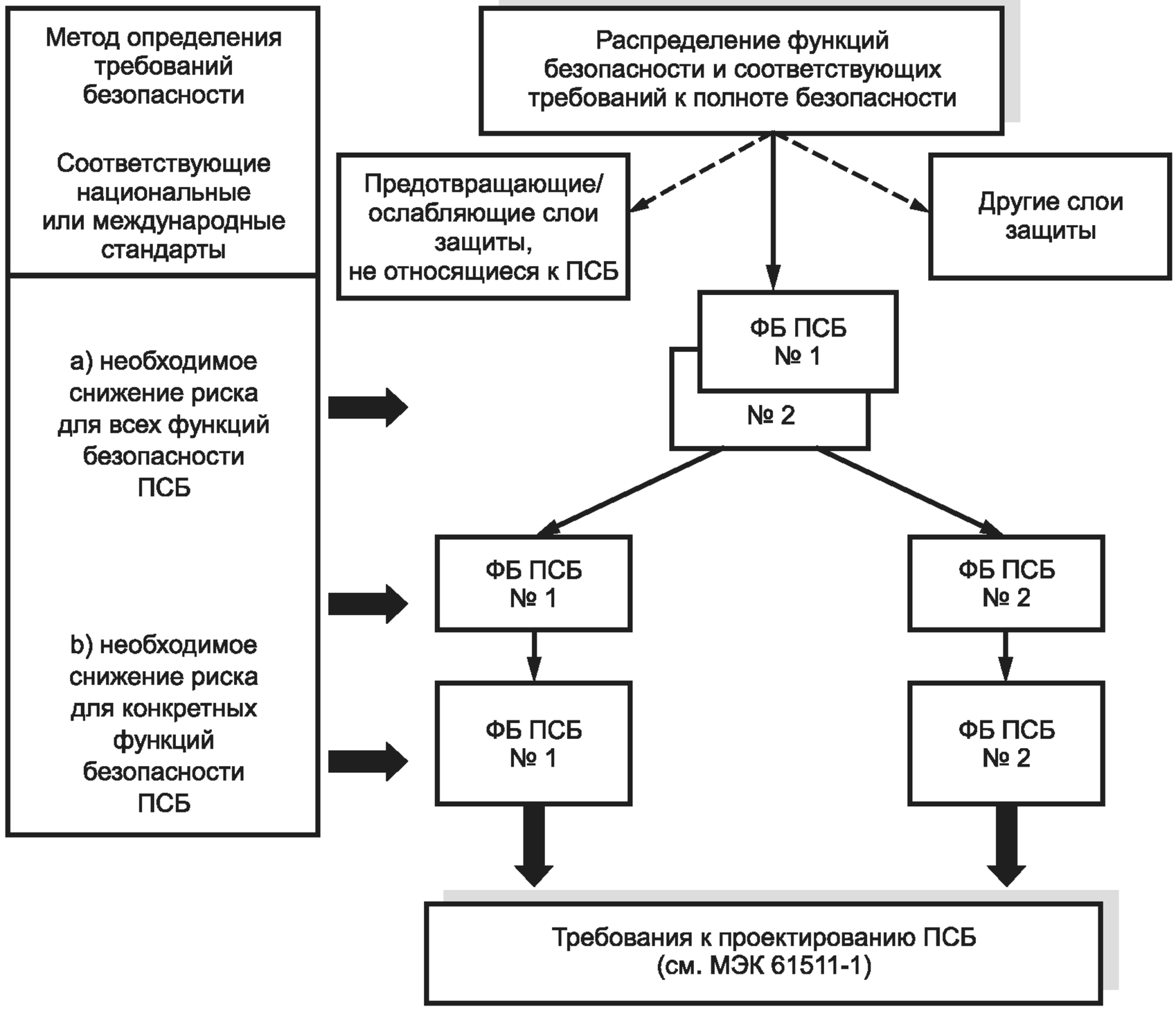


Рисунок 4 — Концепции риска и полноты безопасности

3.6 Распределение требований к безопасности

На рисунке 5 показано распределение требований к безопасности по различным ПСБ и другим слоям защиты. Требования охватывают как функции безопасности, так и полноту безопасности. Требования к стадии распределения требований к безопасности даны в МЭК 61511-1 (раздел 9).

Применение тех или иных методов для распределения требований полноты безопасности по ПСБ, другим связанным с безопасностью технологическим системам, а также по внешним средствам снижения риска зависит прежде всего от того, каким образом определена степень необходимого снижения риска — количественно или качественно. Эти подходы называют полуколичественными, полукачественными и качественными соответственно (см. приложения B, C, D и F).



Примечание — Требования к полноте безопасности устанавливаются для каждой функции безопасности ПСБ до распределения (см. МЭК 61511-1, раздел 9).

Рисунок 5 — Размещение требований безопасности по ПСБ, по слоям защиты или ослабления, не относящимся к ПСБ, и по другим слоям защиты

3.7 Уровни полноты безопасности

В настоящем стандарте определены четыре уровня полноты безопасности (УПБ), причем УПБ 4 — наивысший, УПБ 1 — низший.

Предельные значения показателей отказов для задания всех четырех УПБ определены в МЭК 61511-1 (таблицы 3 и 4). Установлены два таких параметра: один — для ПСБ, действующих в режиме по запросу, и другой — для ПСБ, работающих в непрерывном режиме.

Примечание — В случае ПСБ, работающей в режиме по запросу, мерой полноты безопасности является средняя вероятность отказа выполнения функции безопасности при появлении запроса. В случае, если ПСБ работает в непрерывном режиме, мерой полноты безопасности является частота опасных отказов функции безопасности в час (см. МЭК 61511-1, пункт 3.2.43).

3.8 Выбор метода для определения требуемого уровня полноты безопасности

Имеются различные пути установления требуемого УПБ для конкретного случая. В приложениях B — F представлена информация о ряде используемых методов. Выбор метода для конкретного применения зависит от многих факторов, в том числе от:

- сложности задачи;
- указаний регулирующих органов;
- природы риска и требуемой величины его снижения;
- опыта и квалификации персонала, выполняющего эту работу;
- доступной информации о параметрах риска.

В некоторых случаях можно использовать не один, а несколько методов. Так, при определении требуемого УПБ для всех рассматриваемых функций безопасности ПСБ в качестве первого шага можно использовать качественные методы. Те функции, которым с помощью этого метода был присвоен УПБ 3 или 4, следует затем проанализировать более детально с использованием количественных методов для получения более точной оценки требуемой их полноты безопасности.

Приложение А
(справочное)

Принцип снижения риска настолько, насколько это практически целесообразно (принцип ALARP), и концепция приемлемого риска

А.1 Общие положения

В данном приложении рассмотрен особый принцип (ALARP), который может быть применен в процессе определения приемлемого риска и УПБ. Принцип ALARP сам по себе — это не метод решения задачи определения УПБ, а концепция, которая может быть применена в процессе решения этой задачи. Желающие использовать практически принципы, указанные в этом приложении, должны обратиться к [1] — [5].

А.2 Модель ALARP

А.2.1 Введение

В 3.2 приведены основные критерии, которые используют для контроля за промышленными рисками, и указано, что соответствующая деятельность должна быть направлена на то, чтобы определить:

a) риск велик настолько, что он вообще неприемлем; или

b) риск незначительный либо может быть сведен до этого уровня; или

c) является ли риск промежуточным между оценками, указанными в перечислениях a) и b), и снижен ли он до самого низкого практичного уровня. При этом «практичность» определяется, с одной стороны, преимуществами, которые влекут за собой снижение уровня риска, и, с другой стороны, стоимостью мероприятий по его снижению.

Согласно перечислению c) принцип ALARP рекомендует снижать риск до уровня «практической целесообразности» или до уровня, который является «настолько низким, насколько он практически целесообразен» (ALARP). Таким образом, если риск попадает в область, ограниченную, с одной стороны, областью неприемлемых уровней риска и областью незначительных уровней — с другой, то применение принципа ALARP приводит к тому, что результирующий риск оказывается приемлемым в конкретной ситуации. Согласно этому подходу риск может попасть в одну их трех областей: в недопустимую, приемлемую и вполне приемлемую (см. рисунок А.1).

Риск, превышающий некоторый уровень, считается недопустимым. Такой риск не может быть признан оправданным при любых нормальных обстоятельствах. Если такой риск существует, то он либо должен быть снижен настолько, чтобы попасть в область приемлемого или вполне приемлемого риска, либо должен быть устранен источник опасности.

Риск ниже этого уровня считается приемлемым при условии, что он был уменьшен до уровня, при котором выгода от дальнейшего его снижения не оправдана ввиду требующихся для этого больших затрат и при условии, что для управления этим риском применены все соответствующие общепринятые стандарты. Чем выше риск, тем обычно больше расходы по его сокращению. Риск, сниженный таким образом, можно рассматривать как «сниженный до практически целесообразного уровня» (ALARP).

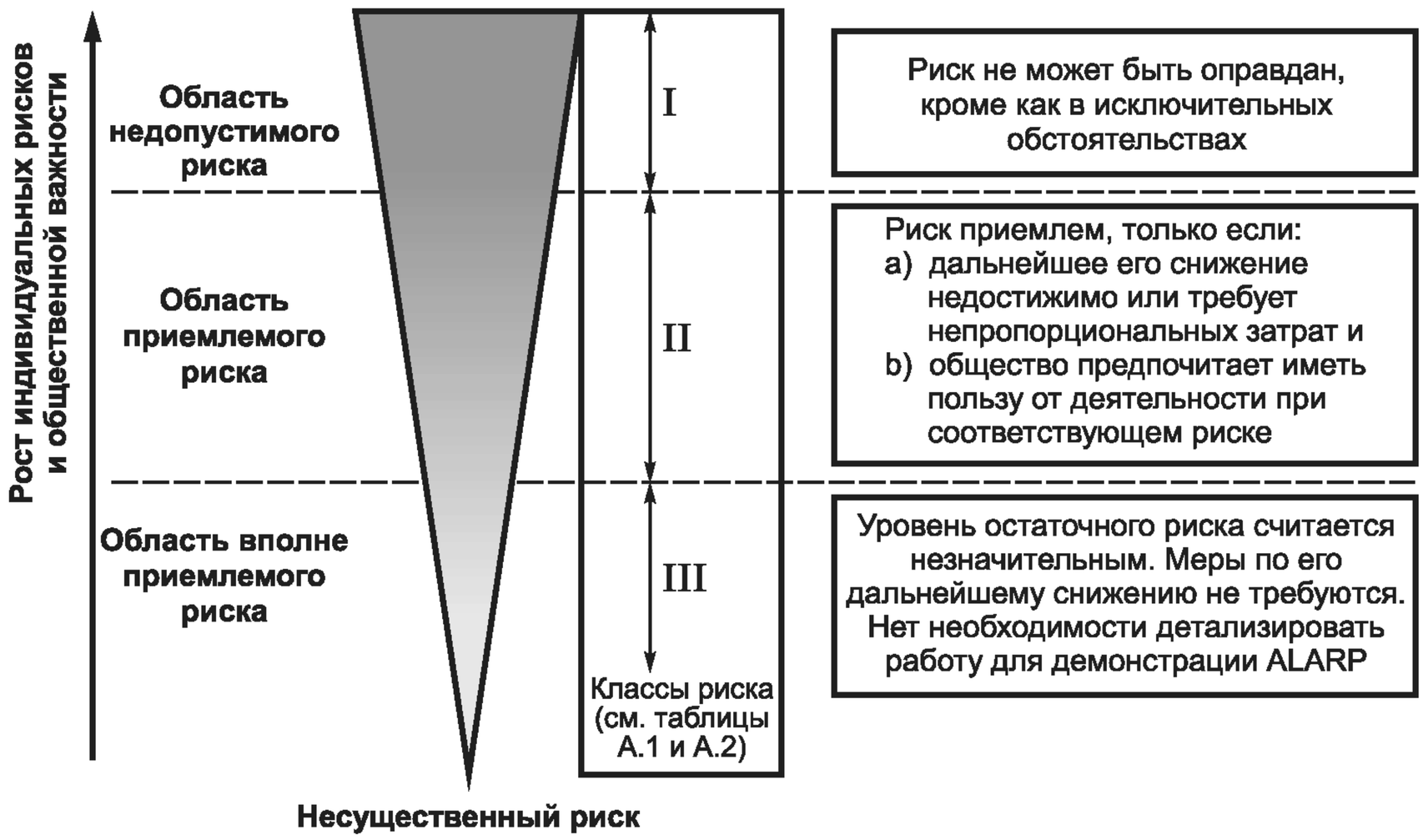


Рисунок А.1 — Приемлемый риск и принцип ALARP

В области, расположенной ниже области допустимых значений, уровни риска считаются настолько несущественными, что контролирующий орган не требует дальнейших улучшений. Эта широкая область, риски в которой малы по сравнению с ежедневно испытываемыми нами рисками, не требует детальных исследований для демонстрации ALARP; однако необходимо сохранять бдительность, чтобы быть уверенным в том, что риск остается на прежнем уровне.

Концепцию ALARP можно применять и при качественном, и при количественном способе задания риска. В А.2.2 рассмотрен метод, используемый при количественном задании риска. (В приложении С приведен полуколичественный метод, а в приложениях D и E — качественные методы определения необходимого снижения риска при конкретном источнике опасности. В рассмотренных методах для принятия решения может быть использована концепция ALARP.)

При применении принципа ALARP необходимо всегда быть уверенным, что все принятые предположения обоснованы и документально оформлены.

А.2.2 Задание приемлемого риска

Для применения принципа ALARP необходимо предварительно определить границы трех областей, показанных на рисунке А.1, значения которых выражены вероятностью возникновения события и его последствиями. Такое определение обычно бывает результатом обсуждения и соглашения между заинтересованными сторонами (например, между регулирующими органами в области безопасности, теми, действия которых приводят к появлению риска, и теми, кто этому риску подвергается).

Чтобы использовать принцип ALARP, надо установить соответствие между последствиями риска и приемлемой частотой его возникновения, что может быть сделано, введя классы риска. В таблице А.1 в качестве примера приведены три класса (I, II, III) для разных частот возникновения риска и разных вариантов его последствий. В таблице А.2 дана интерпретация каждого из классов риска на базе концепции ALARP. Описание каждого из классов риска выполняется на основе рисунка А.1. Подразумевается, что риски, определенные внутри каждого из классов, — это риски, по отношению к которым уже приняты меры по их сокращению. Согласно рисунку А.1 можно выделить следующие три класса рисков:

класс I — недопустимая область;

класс II — область применения концепции ALARP;

класс III — наиболее приемлемая область.

Таблица, подобная таблице 1, обычно создается для каждой конкретной ситуации или для конкретной подотрасли промышленности, принимая во внимание широкий круг социальных, политических и экономических факторов. Каждому виду последствий ставятся в соответствие вероятность и таблица с классами риска. Например, «вполне вероятен» в таблице А.1 может означать событие, которое возникает с частотой, превышающей 10 раз в год. Его критическим последствием может быть один смертельный исход и/или многочисленные телесные повреждения, или несколько случаев профессиональных заболеваний.

Задав допустимый риск, можно определить уровни полноты безопасности функций безопасности ПСБ с помощью, например, одного из методов, описанных в приложениях С — F.

Таблица А.1 — Пример классификации инцидентов

Возможность инцидента	Класс риска			
	Катастрофические последствия	Критические последствия	Незначительные последствия	Пренебрежимо малые последствия
Вполне вероятен	I	I	I	II
Вероятен	I	I	II	II
Возможен	I	II	II	II
Мало вероятен	II	II	II	III
Невероятен	II	III	III	III
Невозможен	II	III	III	III

Примечания

1 Интерпретацию классов риска с I по III см. в таблице А.2.

2 Фактическое заполнение таблицы индексами классов риска I, II и III зависит от конкретной ситуации, а также от того, какие фактические значения вероятности мы присваиваем понятиям «вероятно», «возможно» и т. д. Таким образом, таблицу А.1 следует рассматривать как иллюстрацию того, каким образом подобная таблица может заполняться, а не как вариант для дальнейшего использования.

Т а б л и ц а А.2 — Интерпретация классов риска

Класс риска	Интерпретация
Класс I	Неприемлемый риск
Класс II	Нежелательный риск, допустимый, только если его дальнейшее снижение практически невозможно или если связанные с этим расходы непропорционально велики по сравнению с достигаемым результатом
Класс III	Пренебрежимо малый риск
П р и м е ч а н и е — Связь между УПБ и классом риска отсутствует. УПБ определяется снижением риска, связанным с конкретной функцией безопасности ПСБ (см. приложения B — F).	

Приложение В
(справочное)

Полуколичественный метод

В.1 Общие сведения

В данном приложении рассмотрен вопрос о том, как с помощью полуколичественного подхода можно определять УПБ. Полуколичественный подход наиболее целесообразен в случаях, когда приемлемый риск определяется численно (например, определенные последствия не должны возникать чаще, чем один раз в сто лет).

Данное приложение не предназначено для использования в качестве руководства по применению конкретного метода, а имеет своей целью проиллюстрировать его общие принципы. Приложение основано на методе, детально описанном в [6].

В.2 Соответствие МЭК 61511-1

Общая цель данного приложения — проследить процедуру выбора необходимых функций безопасности ПСБ и установления их УПБ. Для решения этой задачи необходимо выполнить следующие основные шаги:

1) установить целевую (заданную) безопасность процесса (приемлемый риск);
2) провести анализ опасности и риска, чтобы оценить существующий риск;
3) определить требуемую функцию (функции) безопасности;
4) распределить функции безопасности по слоям защиты.

Примечание — Предполагается, что слои защиты не зависят один от другого;

5) определить, требуются ли функции безопасности ПСБ;
6) определить УПБ функций безопасности ПСБ для конкретного слоя защиты.

Шаг 1 определяет требование к безопасности процесса. На шаге 2 выполняется анализ риска процесса, а шаг 3 позволяет на основании анализа риска определить, какие требуются функции безопасности и каким должно быть снижение риска, чтобы заданная безопасность была достигнута. После распределения на шаге 4 этих функций безопасности по слоям защиты становится ясным, требуется ли функция (функции) безопасности ПСБ (шаг 5) и каким должен быть ее (их) УПБ (шаг 6).

В данном приложении предлагается для достижения целей серии стандартов МЭК 61511 использовать при оценивании риска полуколичественные методы. Этот подход продемонстрирован на простом примере.

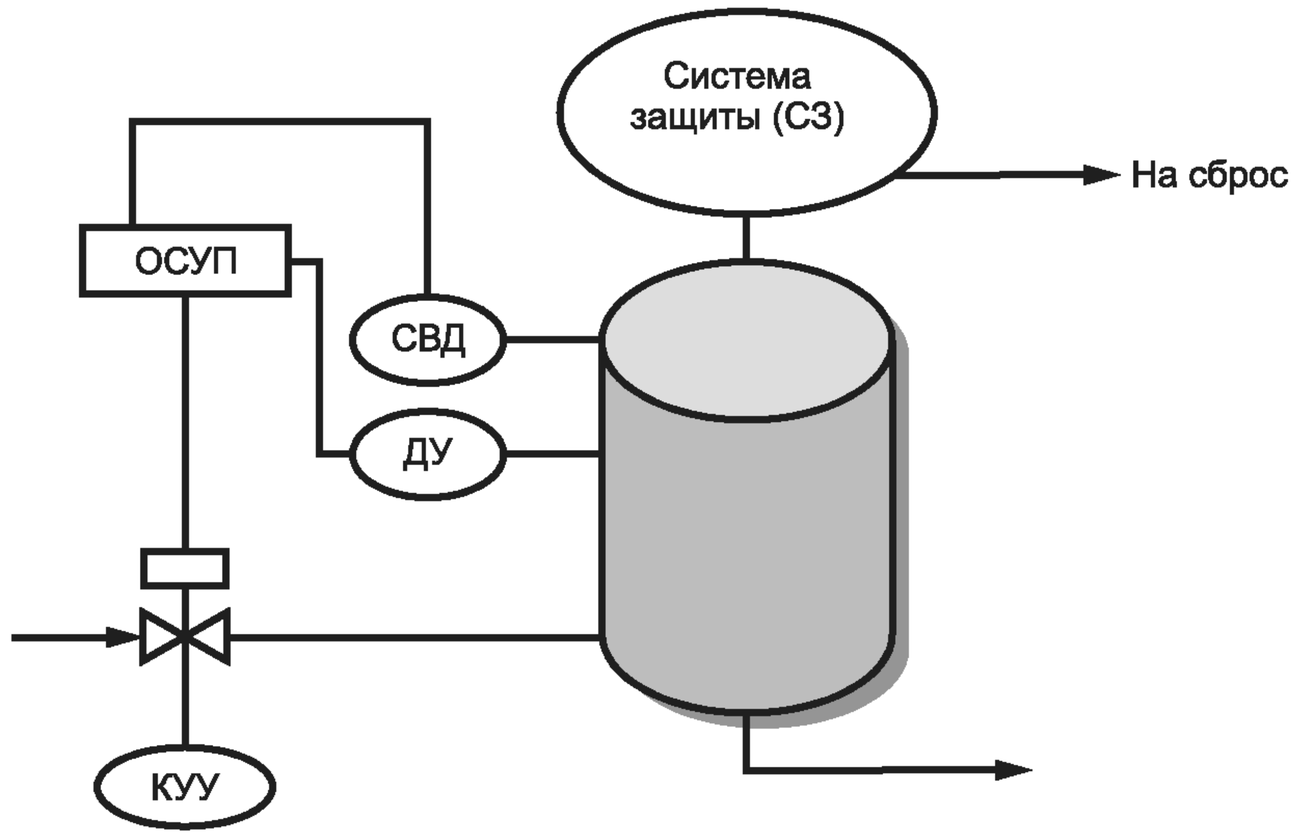
В.3 Пример

Рассмотрим процесс, включающий емкость под давлением с летучей воспламеняющейся жидкостью и необходимое оборудование (см. рисунок В.1). Управление объектом осуществляется основной системой управления процессом (ОСУП), которая контролирует сигнал датчика уровня и управляет перемещением клапана. Имеются следующие технические системы, реализующие процесс: а) независимый датчик давления, который в случае недопустимого повышения давления выдает предупредительный сигнал, побуждающий оператора к принятию соответствующих мер по прекращению подачи жидкости в емкость, и б) если реакции оператора на аварийный сигнал не последует, включается дополнительный неприборный слой защиты от повышения давления. Выбросы с помощью системы защиты отводятся по трубам в сепараторную емкость, которая соединена с системой сброса газа. В этом примере принимается, что система сброса газа спроектирована, смонтирована и действует нормально и имеет разрешение на применение. Таким образом, потенциально возможные отказы системы сброса газа в этом примере не рассмотрены.

Примечание — Понятие «технические системы» относится здесь ко всем системам, работающим с процессом. Они включают и иные автоматические средства защиты, а также оператора (операторов).

В.3.1 Заданный уровень безопасности процесса

Фундаментальным условием успешного управления промышленным риском является четкое и ясное определение заданного уровня безопасности процесса (приемлемого риска). Он может быть установлен на базе национальных и международных стандартов и правил, корпоративной политики, а также под влиянием заинтересованных сторон, таких как сообщества и/или местные органы и страховые компании с хорошей технической подготовкой. Заданный уровень безопасности процесса специфичен для конкретного процесса, корпорации или отрасли. Таким образом, обобщения невозможны, за исключением ситуаций, когда существующие правила и стандарты обеспечивают поддержку таким обобщениям. В качестве примера примем, что для задания безопасности процесса установлено, что средняя частота сброса не должна превышать 10^{-4} в год, что объясняется ожидаемыми последствиями сброса для окружающей среды.



СЗ — система защиты для дополнительного ослабления последствий (сток, сброс давления, ограниченное пространство, резервная емкость); СВД — сигнализатор высокого давления; ДУ — датчик уровня; КУУ — клапан управления уровнем; ОСУП — основная система управления процессом

Рисунок В.1 — Емкость под давлением с существующими системами безопасности

В.3.2 Анализ опасности

Для того чтобы выявить опасности, возможные отклонения процесса и их причины, исходные события и потенциально опасные события (инциденты) в используемых технических системах, следует провести анализ опасностей процесса. Для этого могут быть использованы следующие методы качественного анализа:

- анализ безопасности;
- контрольные листы;
- анализ гипотез («что произойдет, если»);
- метод HAZOP;
- анализ видов и последствий отказов;
- анализ причин и последствий.

Одним из таких методов, получивших широкое применение, является метод анализа опасности и работоспособности (Hazard and Operability, HAZOP). Анализ (или изучение) опасности и работоспособности выявляет и оценивает опасности для технологической установки, а также другие неопасные проблемы, связанные с работоспособностью, которые ставят под сомнение возможность достижения проектной производительности установки.

На втором шаге для примера, приведенного на рисунке В.1, проводится анализ HAZOP. Целью применения этого метода анализа является оценка потенциально опасных событий, связанных с выбросами в окружающую среду. Краткий перечень результатов применения метода приведен в таблице В.1.

В результате применения HAZOP установлено, что значительное превышение давления может привести к выбросам горючего материала в окружающую среду. Это является исходным событием, которое может перерасти в опасное событие по сценарию, зависящему от реакции имеющихся технических систем. Если бы метод HAZOP был применен к анализу объекта в полной мере, то в рассмотрении могли бы появиться иные исходные события, приводящие к выбросам, включая утечку из технологического оборудования, полный разрыв трубопровода и такие внешние события, как пожар. В данном иллюстративном примере рассмотрены только условия возникновения высокого давления.

Таблица В.1 — Результаты анализа методом HAZOP

Объект	Отклонение	Причины	Последствия	Защита	Действие
Емкость	Высокий уровень	Отказ ОСУП	Высокое давление	Оператор	
	Высокое давление	1 Высокий уровень. 2 Внешнее возгорание	Выброс в окружающую среду	1 Сигнализация, оператор, слой защиты. 2 Система пожаротушения	Оценка условий выброса в окружающую среду

Окончание таблицы В.1

Объект	Отклонение	Причины	Последствия	Защита	Действие
	Малый поток/ отсутствие потока	Отказ ОСУП	Нет последствий, представляющих интерес		
	Обратный поток		Нет последствий, представляющих интерес		

В.3.3 Полуколичественный метод анализа риска

Оценку рисков процесса выполняют с помощью полуколичественного метода анализа, который позволяет определить и количественно оценить риски, связанные с возможными ошибками или опасными событиями в технологическом процессе. Результаты анализа могут быть использованы для выбора необходимых функций безопасности и их УПБ, дающих возможность снизить риск процесса до приемлемого уровня. Оценка риска процесса с помощью полуколичественного способа может быть выполнена в виде приведенной ниже последовательности шагов, причем первые четыре шага могут быть реализованы в процессе применения метода HAZOP:

1 Выделить опасности для процесса.

2 Определить состав слоев защиты.

Примечания

1 Слои защиты включают совокупность всех систем безопасности, предназначенных для защиты процесса, включая ПСБ, системы, связанные с безопасностью, основанные на других технологиях, внешние средства снижения риска и реакцию оператора.

2 Шаг 2 применяется, так как это действующий процесс, как в рассмотренном примере.

3 Определить исходные события.

4 Построить сценарии опасного развития событий применительно к каждому исходному событию.

5 С помощью архивных данных или используя методы моделирования (анализ дерева ошибок, методы Маркова), уточнить частоту появления исходных событий и надежность существующих систем безопасности.

6 Оценить количественно частоту возникновения всех существенно опасных событий.

7 Оценить последствия всех существенно опасных событий.

8 Просуммировать результаты (последствия и частоту инцидентов) оценки риска, связанного с каждым опасным событием.

Существенные результаты такого анализа, представляющие интерес:

- лучшее и более детальное понимание опасностей и рисков, связанных с процессом;
- знание риска процесса;
- понимание вклада имеющихся систем безопасности в общее снижение риска;
- определение каждой функции безопасности, требующейся для снижения риска процесса до приемлемого уровня;
- сравнение полученной оценки риска процесса с заданным значением.

Способ полуколичественного анализа требует значительных ресурсов, но имеет достоинства, которые не обеспечивают качественные подходы. При определении опасностей этот способ базируется в большой степени на экспертных оценках команды специалистов, обеспечивает ясный способ управления существующими системами безопасности, основанными на других технологиях, использует средства документирования всех мероприятий, которые привели к полученным результатам, и обеспечивает поддержку жизненного цикла.

Для представленного примера с помощью HAZOP анализа было идентифицировано одно исходное событие (возникновение избыточного давления), которое повлекло возникновение возможности выброса вещества в окружающую среду. Необходимо отметить, что используемый в данном пункте подход является комбинацией количественной оценки частоты возникновения опасного события и качественной оценки его последствий. Данный подход применяют для иллюстрации систематической процедуры, которой рекомендуется следовать для определения опасных событий и функций безопасности ПСБ.

В.3.4 Анализ рисков существующих процессов

Следующий шаг состоит в установлении факторов, которые могут способствовать возникновению исходного события. На рисунке В.2 показано простое дерево ошибок, на котором представлен ряд причин возникновения чрезвычайно высокого давления в емкости. Событие верхнего уровня — чрезмерное повышение давления в емкости — может быть вызвано отказом ОСУП или внешним фактором — пожаром (см. таблицу В.1). Дерево ошибок наглядно представляет воздействие отказа ОСУП на процесс. Сама ОСУП не выполняет каких-либо функций защиты. Ее отказ, однако, приводит к росту числа запросов к ПСБ. Таким образом, при наличии надежной ОСУП запросов к ПСБ было бы меньше. Дереву ошибок можно поставить в соответствие количественные оценки. В настоящем примере предполагается, что частота появления условий чрезвычайно высокого давления имеет порядок 10^{-1} в год.

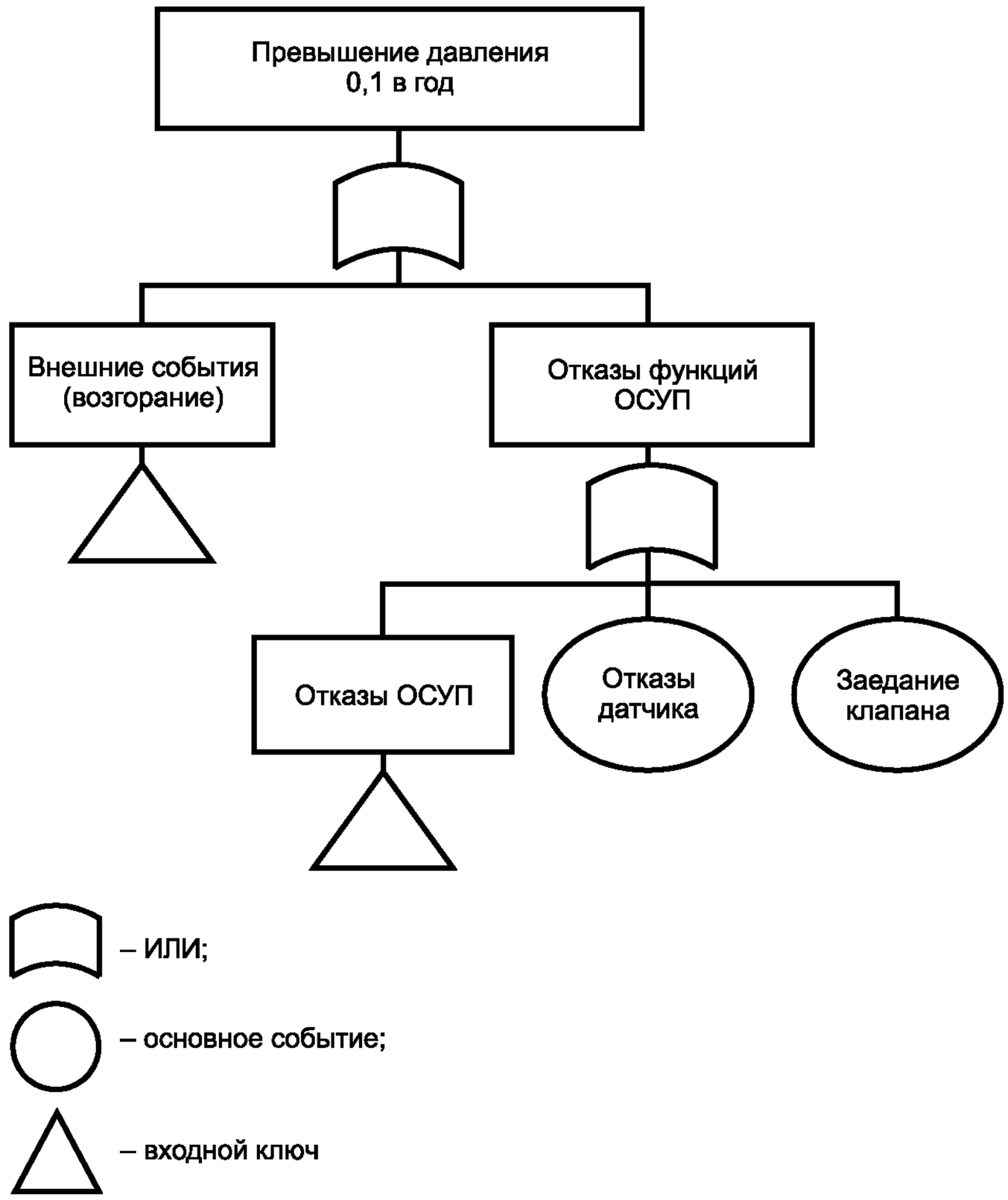


Рисунок В.2 — Дерево неисправностей при превышении давления в емкости

После установления частоты появления исходного события, используя средства анализа дерева событий, проводят моделирование реакции систем безопасности (успешная работа или отказ) на аномальные условия. Данные по надежности систем безопасности могут быть взяты из эксплуатационных данных, опубликованных баз данных или получены по результатам прогноза методом моделирования надежности. Для рассматриваемого примера использованы реальные данные, а не данные, взятые из литературы или полученные в результате прогнозирования работы системы.

На рисунке В.2 показаны возможные сценарии потенциального выброса, которые могут произойти в условиях повышения давления. В результате моделирования таких случаев были получены: a) частота возникновения каждой из приводящих к аварии последовательности событий и b) качественная оценка последствий в виде выброса воспламеняющихся материалов.

На рисунке В.3 показаны пять вариантов развития опасных событий, причем для каждого приведены частота появления и последствия возможного выброса. При аварии по сценарию 1 выбросы отсутствуют. Такая авария соответствует исходным условиям, принятым при проектировании процесса. Более того, условиям проектирования соответствуют также случаи «опасных» сценариев 2 и 4, при которых происходит выброс материала для вспышки. Частота возникновения аварий для сценариев 3 и 5, для которых характерен выброс материала в окружающую среду, находится в пределах от 9×10^{-4} до 1×10^{-3} в год.

Примечание — Предполагается, что события, изображенные на рисунке В.3, независимы. Более того, указанные данные являются приближенными, поэтому сумма частот всех возникающих аварий приближается к частоте исходного события (0,1 в год).

Следует отметить, что при анализе не принималась во внимание возможность отказа по общей причине сигнализатора высокого давления и отказа датчика уровня в составе ОСУП. Такого рода отказы по общей причине могут привести к существенному увеличению вероятности отказов системы аварийной сигнализации при наличии запроса и, следовательно, увеличить риск. Для получения дополнительной информации см. [7].

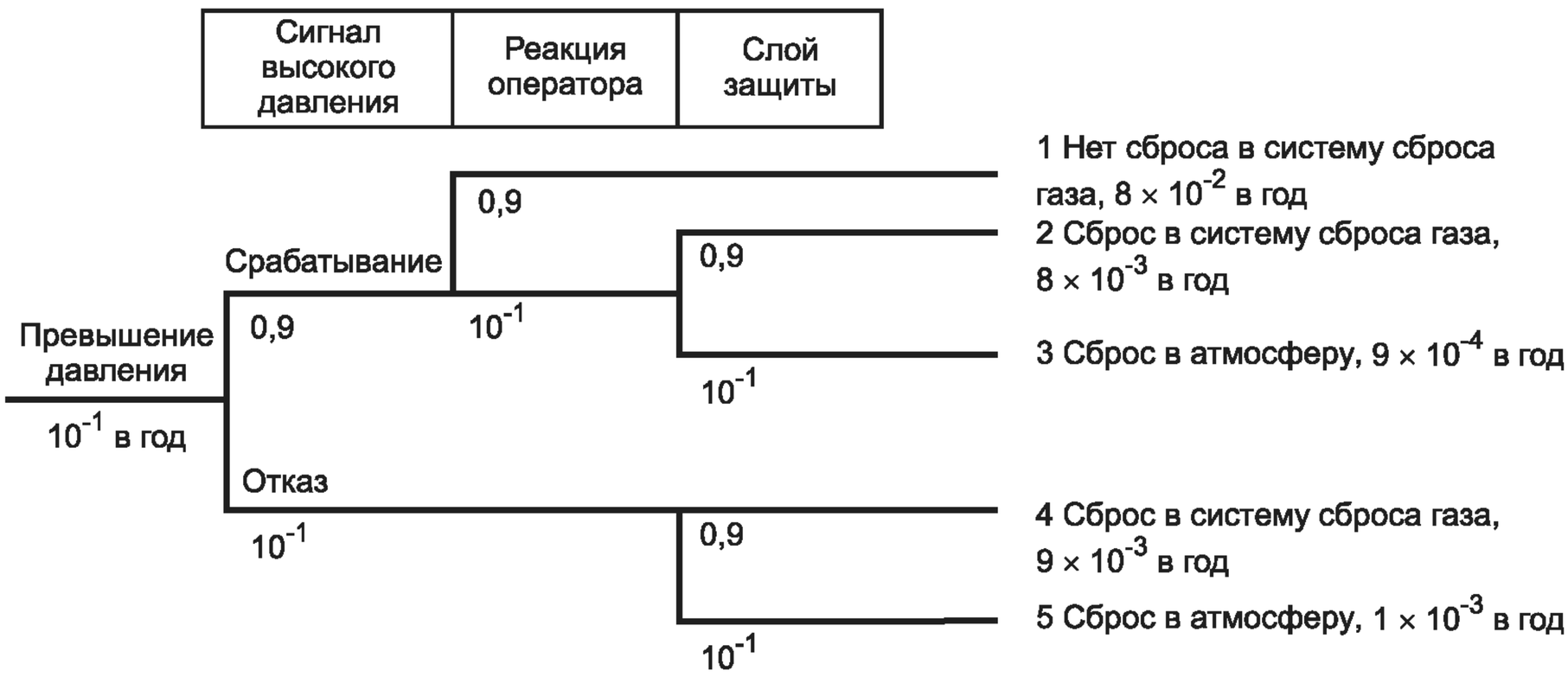


Рисунок В.3 — Опасные события при существующих системах безопасности

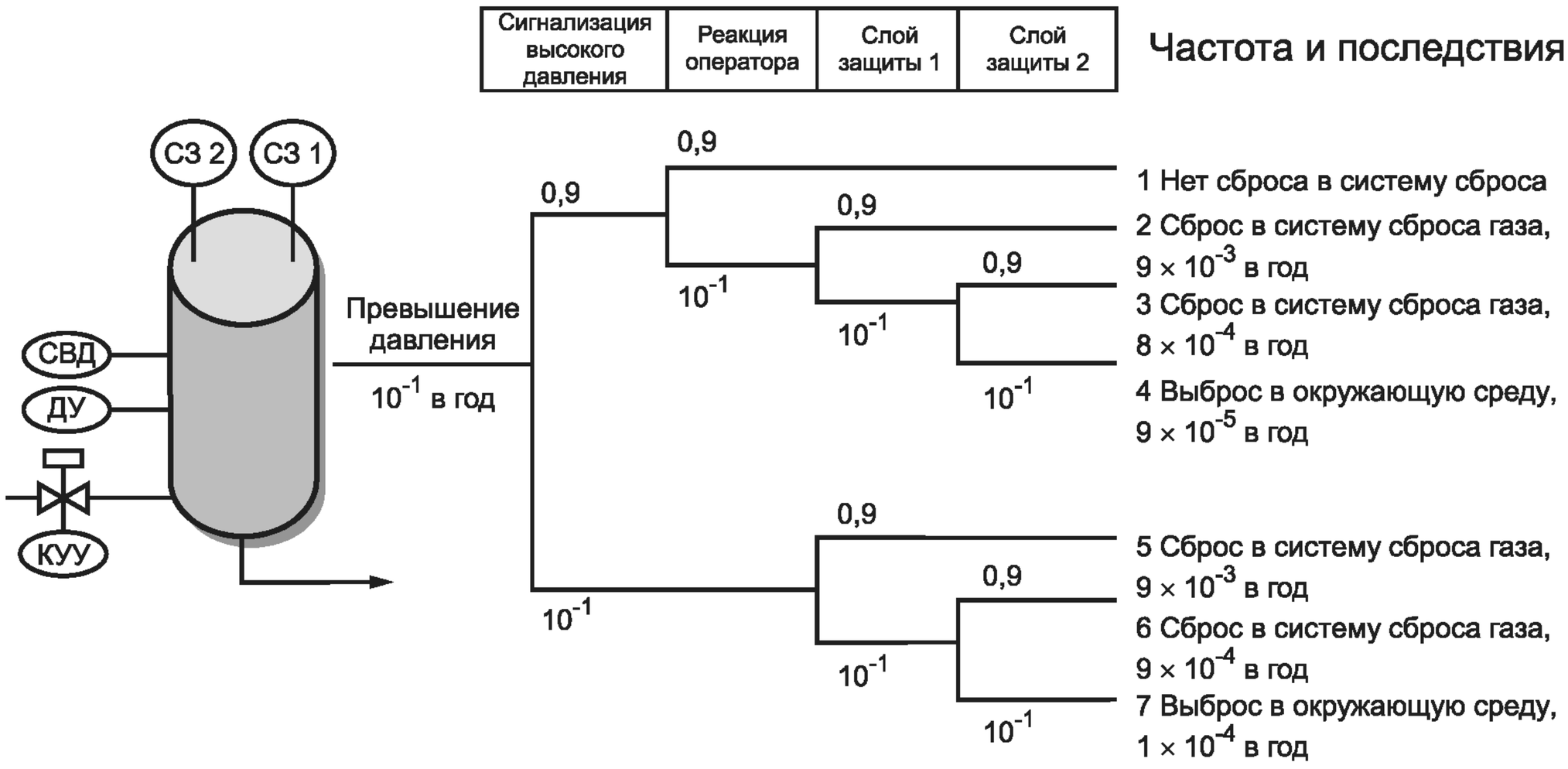
В.3.5 События, не отвечающие заданному уровню безопасности

Как отмечалось ранее, специфическое требование технологического объекта состоит в том, чтобы установить следующее задание на уровень безопасности: выброс материала в окружающую среду должен происходить с частотой, не превышающей 10^{-4} раз в год. Для того чтобы выполнить это задание при данной частоте появления опасных событий и их последствиях (рисунок В.3), необходимо снизить риск так, чтобы аварийные ситуации по сценариям 3 и 5 отвечали заданному уровню безопасности.

В.3.6 Снижение риска с помощью других слоев защиты

Прежде чем установить необходимость выполнения функции безопасности ПСБ, следует рассмотреть слои защиты, использующие другие технологии. Чтобы проиллюстрировать эту процедуру, примем, что в целях дальнейшего усиления действия существующей системы безопасности вводится еще один дополнительный совершенно независимый слой защиты. Процесс с новым слоем защиты показан на рисунке В.4. Для выявления всех потенциально опасных событий используют метод дерева событий. Из рисунка В.4 следует, что в условиях превышения давления могут произойти семь видов аварийных событий с выбросом материала.

Анализ частоты появления моделируемых опасных событий, отображенных на рисунке В.4, показывает, что заданный для емкости уровень безопасности не достигается в случаях опасных событий 4 и 7, когда имеет место выброс материала в окружающую среду, и, следовательно, уровень безопасности ниже заданного. Фактически об-



СЗ 1 — слой защиты; СЗ 2 — слой защиты 2; СВД — сигнализатор высокого давления; ДУ — датчик уровня; КУУ — клапан управления уровнем

Рисунок В.4 — Опасные события при резервированном слое защиты

щая частота выбросов в окружающую среду составляет $1{,}9 \times 10^{-4}$ раз в год. На этой стадии следует оценить целесообразность использования внешних средств снижения риска. Принимая, что цель обеспечения безопасности — минимизировать риск, связанный с выбросами в окружающую среду, можно заключить, что использование таких внешних средств снижения риска, как ограждение, не является целесообразным альтернативным способом уменьшения риска. Таким образом, поскольку никакая иная не входящая в ПСБ защита не может обеспечить заданный уровень безопасности, то для защиты от превышения давления и выброса воспламеняющегося материала требуется функция безопасности, выполняемая ПСБ.

В.3.7 Снижение риска путем использования функции безопасности ПСБ

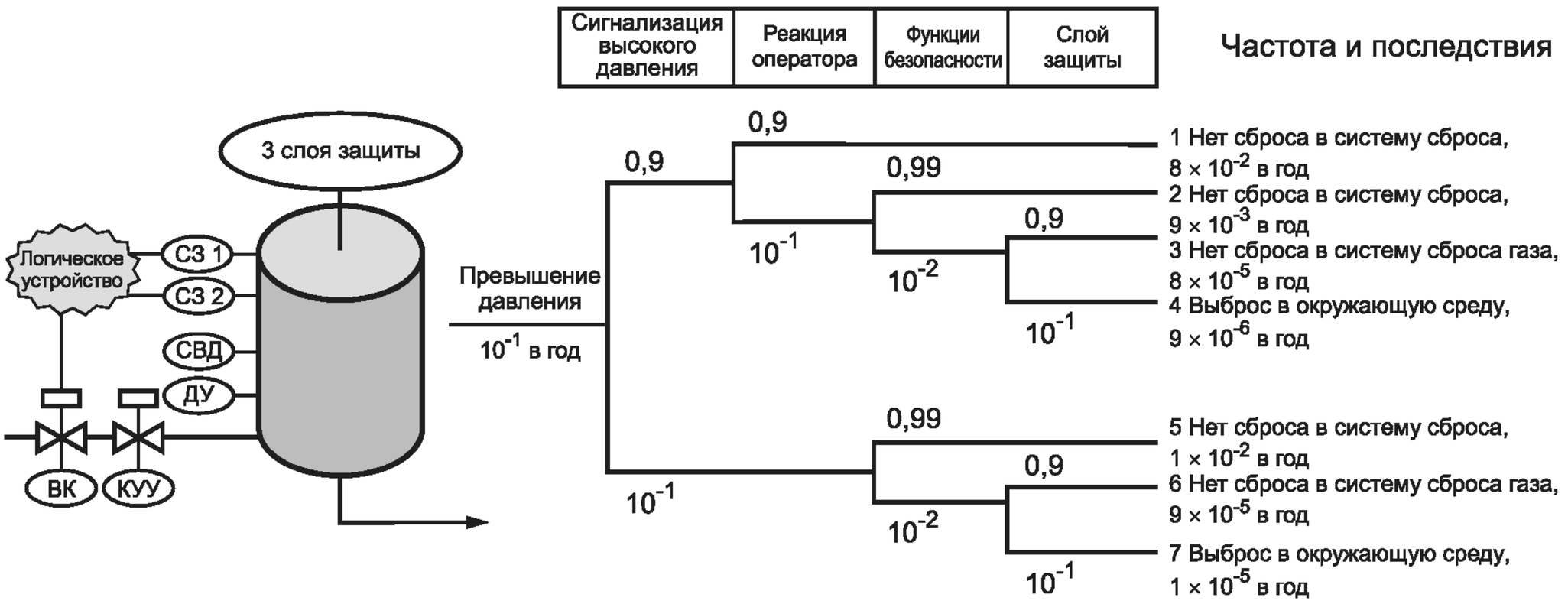
Заданного уровня безопасности не удается достигнуть с помощью применения слоев защиты, использующих иные технологии, или внешних средств снижения риска. Сценарий 7, при котором может произойти выброс, сам по себе еще соответствует заданию безопасности. Фактически же суммарная частота выбросов в окружающую среду, как следует из рисунка В.4, составляет $1{,}9 \times 10^{-4}$ в год (сумма частот по сценариям 4 и 7). Для уменьшения общей частоты выбросов в атмосферу (т. е. чтобы обеспечить соответствие заданию по безопасности) в ПСБ требуется реализовать новую функцию безопасности с УПБ 2. Новая функция безопасности ПСБ показана на рисунке В.5. На этом этапе нет необходимости в детальной разработке функции безопасности ПСБ, достаточно лишь ее общее концептуальное решение. Цель этого шага — установить, обеспечит ли выполнение функции безопасности ПСБ с УПБ 2 требуемое снижение риска и позволит ли это достигнуть заданного уровня безопасности. Детальное проектирование функции безопасности ПСБ следует выполнить только после того, как будет достигнут заданный уровень безопасности. Например, в новой функции безопасности ПСБ может быть использован сдвоенный датчик давления, включенный по схеме 1oo2 (1 из 2) и связанный с логическим решающим устройством, которое управляет дополнительным отсечным клапаном.

Примечание — Обозначение 1oo2 означает «один из двух», т. е. любой из сдвоенных датчиков может послать сигнал, останавливающий процесс.

Новая функция безопасности ПСБ с УПБ 2 предназначена для уменьшения частоты выбросов из сосуда, находящегося под высоким давлением. На рисунке В.5 изображен новый слой защиты и представлены все потенциально опасные сценарии. Как можно видеть на этом рисунке, частота выбросов из такой емкости может быть снижена до значения 10^{-4} в год и ниже и заданный уровень безопасности может быть достигнут при условии, что полученная в результате функция безопасности ПСБ отвечает требованиям УПБ 2. Общая частота выбросов в окружающую среду (сумма частот сценариев 4 и 7) снижена до $1{,}9 \times 10^{-5}$ в год, ниже критерия безопасности, равного 10^{-4} в год.

Следует отметить, что анализ с использованием дерева событий не учитывает возможность появления отказа по общей причине в системе аварийной сигнализации высокого давления и функции безопасности ПСБ с УПБ 2. Возможен также отказ по общей причине обоих этих защитных устройств и датчика уровня в составе ОСУП.

Такие отказы по общей причине приводят к существенному увеличению вероятности отказа защитных функций при наличии запроса и, следовательно, к значительному увеличению общего риска. Для получения дополнительной информации см. [7].



СЗ 1 — система защиты; СЗ 2 — система защиты; СВД — сигнализатор высокого давления; ДУ — датчик уровня; ВК — входной клапан; КУУ — клапан управления уровнем

Рисунок В.5 — Опасные события при функции безопасности ПСБ с УПБ 2

Приложение С
(справочное)

Метод матрицы слоев безопасности

С.1 Введение

Для каждого технологического процесса снижение риска должно начинаться уже на стадии проектирования процесса при выборе наиболее важных решений: при выборе собственно процесса и его местоположения, при принятии решения о запасах опасных реагентов и их размещении. Минимизация запасов опасных химических компонентов, применение таких трубопроводных и теплообменных систем, которые физически исключают нежелательное смешивание активных химических веществ, выбор толстостенных сосудов, способных противостоять максимально возможным давлениям в процессе, выбор теплоносителя, максимальная температура которого ниже температуры разложения реагентов, — все эти проектные решения по процессу снижают эксплуатационные риски. Такое внимание к снижению риска путем тщательного выбора конструктивных и технологических параметров процесса — это ключ к созданию безопасного процесса. Рекомендуется и в дальнейшем продолжать поиски путей снижения опасности и применения заведомо безопасных проектных решений. К сожалению, даже используя в максимальной степени эту философию проектирования, не удается полностью исключить потенциальную опасность и приходится применять дополнительные защитные меры.

В промышленных технологических процессах для их защиты применяют многочисленные слои защиты (СЗ), как это показано на рисунке С.1. Каждый СЗ, показанный на этом рисунке, состоит из специального оборудования и/или элементов административного управления, которые, действуя совместно с другими СЗ, уменьшают риск процесса и/или управляют им.

Концепция слоев защиты базируется на трех основных принципах [8] — [11]:

1) слой защиты представляет собой совокупность технических средств и/или организационных мер, которые функционируют в согласии с другими СЗ, обеспечивая снижение риска процесса или управление им;

2) слой защиты (СЗ) должен удовлетворять следующим критериям:

- снижать определенный риск по меньшей мере в 10 раз,
- обладать такими важными характеристиками, как:
  - специфичность. СЗ проектируется для того, чтобы предотвратить или ослабить последствия одного потенциально опасного события. Причин возникновения этого опасного события может быть много, и, следовательно, действие СЗ может быть вызвано многими исходными событиями;

Рисунок С.1 — Слои защиты

- независимость. СЗ считается независимым от других слоев защиты, если можно показать, что потенциально возможные совместные отказы по общей причине или общего типа отсутствуют;
- надежность. Можно рассчитывать, что СЗ будет выполнять предназначенные для него функции, если при его проектировании учитываются как случайные, так и систематические отказы;
- проверяемость. СЗ проектируется для того, чтобы облегчить регулярное подтверждение соответствия функций защиты;

3) слой защиты, обеспечиваемый функцией безопасности ПСБ, — это такой СЗ, реализация которого удовлетворяет принятому в данном приложении определению ПСБ. (Термин ПСБ был использован при разработке матрицы СЗ).

Заданный уровень безопасности процесса

Фундаментальным условием успешного управления промышленным риском является четкое и ясное определение задаваемого уровня безопасности процесса (приемлемого риска). Он может быть установлен на базе национальных и международных стандартов и правил, корпоративной политики, а также под влиянием заинтересованных сторон, таких как сообщества и/или местные органы и страховые компании с хорошей технической подготовкой. Заданный уровень безопасности процесса специфичен для конкретного процесса, корпорации или отрасли. Таким образом, обобщения невозможны, за исключением ситуаций, когда существующие правила и стандарты обеспечивают поддержку таким обобщениям.

С.2 Анализ опасности

Для того чтобы выявить опасности, возможные отклонения процесса и их причины, исходные события и потенциально опасные события (инциденты) в используемых технических системах, следует провести анализ опасностей процесса. Для этого могут быть использованы следующие методы качественного анализа:

- анализ безопасности;
- контрольные листы;
- анализ гипотез («что произойдет, если»);
- метод HAZOP;
- анализ видов и последствий отказов;
- анализ причин и последствий.

Одним из таких методов, получивших широкое применение, является метод анализа опасности и работоспособности (Hazadr and Operability, HAZOP). Анализ (или изучение) опасности и работоспособности выявляет и оценивает опасности для технологической установки, а также другие неопасные проблемы, связанные с работоспособностью, которые ставят под сомнение возможность достижения проектной производительности установки.

Хотя метод HAZOP первоначально разрабатывался для оценки новых проектов и/или случаев применения, по которым в промышленности было мало опыта, подход оказался весьма эффективным и для действующих процессов. Применение этого метода требует детальных знаний и понимания вопросов проектирования объекта, его функционирования и обслуживания. Обычно опытный руководитель осуществляющей анализ группы специалистов, выполняя процесс разработки, постоянно «ведет» свою команду, используя при этом соответствующий набор подсказок. Такие подсказки применяются в особые или ключевые моменты исследования объекта с учетом соответствующих параметров процесса. Все это позволяет обнаружить возможные отклонения от нормального функционирования процесса. Контрольные листы или опыт выполнения процесса также помогают группе исследователей составить необходимый перечень возможных отклонений, который подлежит рассмотрению в процессе анализа. В результате анализа группа составляет перечни возможных причин отклонений в процессе, последствий таких отклонений, а также необходимых организационных и технических систем. Если причины и последствия отклонений в процессе существенны, а имеющиеся средства защиты недостаточны, то группа может представить на рассмотрение руководства предложения по дополнительным мерам безопасности или по перечню последующих действий.

Часто оказывается возможным обобщить приобретенный на конкретном объекте опыт и результаты его исследования методом HAZOP и распространить все это на имеющиеся в компании аналогичные процессы. Если такое обобщение возможно, то применение метода матрицы слоев безопасности оказывается целесообразным и при ограниченных ресурсах.

С.3 Метод анализа риска

После того как анализ по методу HAZOP проведен, связанный с процессом риск можно оценить, используя как количественные, так и качественные методы. В основе этих методов лежат экспертные оценки, сделанные персоналом предприятия и другими специалистами в области анализа опасности и риска, позволяющие выявить потенциально опасные события и оценить их возможность, интенсивность и последствия.

Для оценки риска процесса может быть использован качественный подход, который позволяет проследить сценарий развития опасного события и оценить его вероятность (примерный диапазон возможности появления) и тяжесть.

Типичное руководство по оценке возможности появления опасных событий без учета действующих СЗ показано в таблице С.1. Данные, приведенные в таблице, носят общий характер и могут быть использованы в тех случаях, когда сведения о конкретном процессе или производстве отсутствуют. Однако если такие конкретные данные имеются, то именно их следует использовать для установления возможности появления опасных событий.

Аналогично в таблице С.2 показан один из способов ранжирования тяжести воздействия опасных событий при их относительном оценивании. Предложенные рейтинги также являются иллюстративными. Тяжесть воздействия опасных событий и их рейтинги строятся для конкретного предприятия (процесса) на базе экспертных оценок и имеющегося опыта.

Таблица С.1 — Частота возможности появления опасного события (без учета СЗ)

Тип события	Возможность возникновения Качественное ранжирование
Множественные отказы различных приборов или клапанов, множественные ошибки персонала при нормальных внешних условиях или спонтанные отказы технологического оборудования	Низкая
Отказы резервированных приборов, клапанов или большие выбросы в зонах загрузки/разгрузки	Средняя
Утечки в процессе, отказы отдельных приборов или клапанов, ошибки персонала, приводящие к небольшим выбросам опасных материалов	Высокая
Примечание — Считается, что система соответствует настоящему стандарту, если утверждается, что отказ функции управления происходит реже чем 10^{-1} в год.	

Таблица С.2 — Критерии ранжирования тяжести воздействия опасных событий

Ранг тяжести	Результат
Обширное	Значительный ущерб оборудованию. Остановка процесса на длительное время. Катастрофические последствия для персонала и окружающей среды
Серьезное	Ущерб оборудованию. Кратковременная остановка процесса. Серьезные последствия для персонала и окружающей среды
Незначительное	Незначительный ущерб оборудованию. Отсутствие остановки процесса. Малый ущерб для персонала и окружающей среды

С.4 Матрица слоев безопасности

Для оценки риска можно использовать матрицу риска, объединяющую вероятность появления опасных событий и рейтинг тяжести их воздействия. Аналогичный подход можно применить и для построения матрицы, которая бы определяла потенциальное снижение риска, связанное с используемой ПСБ для слоя защиты. Подобная матрица риска показана на рисунке С.2, на котором в матрицу был введен заданный уровень безопасности. Иными словами, матрица базируется на конкретном опыте эксплуатации и критериях риска, принятых в данной компании, на принятых в этой компании принципах разработки, эксплуатации и защиты, а также на значении уровня безопасности, установленном компанией в качестве заданного уровня безопасности.

Общее число СЗ включает все СЗ, защищающие процесс, в том числе и классифицируемые ПСБ.

Возможность появления опасного события — это возможность того, что опасное событие произойдет при отключенных СЗ. В качестве руководящего указания см. таблицу С.1.

Тяжесть опасного события — воздействие, связанное с опасным событием. В качестве руководства см. таблицу С.2.

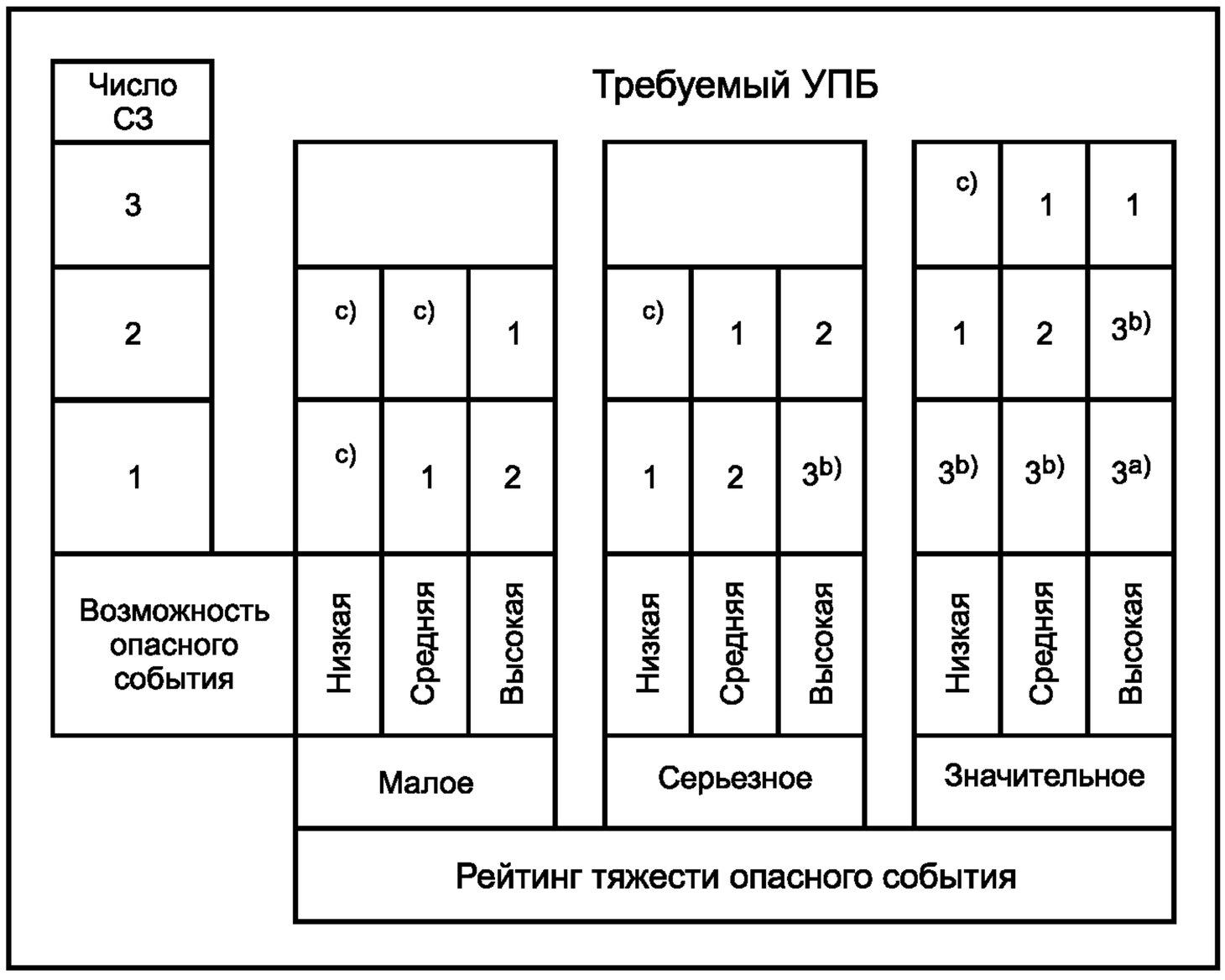
С.5 Общая процедура:

1) установить задание на УПБ процесса;

2) провести анализ возможных опасностей (например, методом HAZOP), чтобы выявить все опасные события, представляющие интерес;

3) построить сценарий развития опасного события и оценить возможность появления этого события, пользуясь при этом данными и руководящими материалами конкретной фирмы;

4) пользуясь руководящими материалами компании, установить рейтинг тяжести опасных событий;



a) Одна функция безопасности ПСБ с УБП 3 не обеспечивает при таком уровне риска достаточного его снижения. Чтобы снизить риск, требуются дополнительные изменения в процессе [(см. перечисление d)].

b) Одна функция безопасности ПСБ с УБП 3 может не обеспечить при таком уровне риска достаточного его снижения. Требуется дополнительный критический анализ [(см. перечисление d)].

c) Вероятно, нет необходимости в независимом от ПСБ слое.

d) Такой поход не считается пригодным в случаях с УПБ 4.

Рисунок С.2 — Пример матрицы слоев безопасности

5) определить используемые на объекте СЗ. Оцениваемую возможность появления опасных событий следует снижать в 10 раз для каждого СЗ;

6) определить необходимость применения дополнительного СЗ, реализуемого ПСБ, путем сравнения остаточного риска с величиной заданного УПБ;

7) определить УПБ системы, пользуясь рисунком С.2.

П р и м е ч а н и е — Пользователю следует оценить возможную степень зависимости между СЗ и попытаться минимизировать любые подобные зависимости.

Приложение D
(справочное)

Определение требуемых уровней полноты безопасности. Полукачественный метод. Калиброванный граф риска

D.1 Введение

Данное приложение базируется на общей схеме формирования графа риска, описанной в МЭК 61508-5 (приложение D.4). Данное приложение адаптировано таким образом, чтобы лучше соответствовать потребностям технологических процессов в промышленности.

В приложении описан метод калиброванного графа риска, применяемый для определения УПБ функций безопасности ПСБ. Этот полукачественный метод позволяет при известных факторах риска, связанных с процессом и базовой системой управления, определить УПБ функций безопасности ПСБ.

В принятом подходе используется ряд параметров, которые в совокупности описывают природу опасной ситуации, возникающей в случае отказа ПСБ или при ее отсутствии. В каждом из четырех наборов параметров выбирается по одному. Выбранные параметры затем объединяются, чтобы решить, какому уровню полноты безопасности должны соответствовать функции безопасности ПСБ. Эти параметры:

- позволяют получить ранжированную оценку рисков и
- представляют собой ключевые факторы оценки риска.

Подход, связанный с применением графа риска, может быть также использован для определения необходимости снижения риска в случае, когда последствия связаны с существенным ущербом для окружающей среды или с материальными потерями. Цель данного приложения – предложить руководство по применению метода.

Сначала в приложении рассматриваются вопросы защиты персонала от опасности. Представлена одна из возможностей применения к технологическому процессу общего графа риска, приведенного в МЭК 61508-5 (рисунок D.1). В заключение, рассматривается применение метода графа риска для защиты окружающей среды и имущества.

D.2 Синтез графа риска

Риск определяется как комбинация вероятности причинения вреда и серьезности этого вреда (см. МЭК 61511-1, раздел 3). Обычно применительно к технологическому процессу риск является функцией следующих четырех параметров:

- последствия опасной ситуации (C);
- заселенность пространства (вероятность того, что в подверженной опасности области находятся люди) (F);
- вероятность того, что опасности можно избежать (P);
- интенсивность запросов (число случаев за год, когда опасная ситуация возникает в отсутствие рассматриваемой функции безопасности ПСБ) (W).

Если граф риска применяется для определения УПБ функции безопасности, выполняемой в непрерывном режиме, то следует рассмотреть необходимость изменения параметров, используемых в графе риска. Такие параметры должны представлять собой факторы риска, которые наилучшим образом соотносятся с характеристиками рассматриваемого объекта. Необходимо также будет рассмотреть соответствие УПБ тем результатам, которые вытекают из решений по выбору параметров, поскольку для снижения риска до допустимого уровня может понадобиться некоторая настройка. Например, параметр W может быть переопределен как общее время работы системы, выраженное в процентах от общего времени ее существования. При таком выборе W1 опасность не является непрерывно действующим фактором и период времени, в котором отказ будет приводить к появлению опасности, будет составлять малую долю года. В этом примере следует пересмотреть и другие параметры, чтобы соответствующие критерии принятия решения и пересмотренные результаты определения УПБ гарантировали допустимость риска.

Таблица D.1 — Описание параметров графа риска для промышленных процессов

Параметр		Описание
Последствия	C	Число жертв и/или серьезных травм, которые, вероятно, появятся в результате опасного события. Определяется путем подсчета числа людей в подвергшейся опасному событию обитаемой области с учетом их уязвимости по отношению к опасному событию
Заселенность	F	Вероятность того, что область, в которой произошло опасное событие, заселена. Определяется путем расчета доли времени, в течение которого область была заселенной, по отношению к времени действия опасного события. При этом следует исходить из большей вероятности нахождения людей в опасной области, что позволит изучить нештатные ситуации, которые могут возникнуть при развитии опасного события (следует также оценить, не приведет ли это к необходимости пересмотра параметра C)

Окончание таблицы D.1

Параметр		Описание
Вероятность того, что опасности можно избежать	P	Вероятность того, что люди могут избежать опасной ситуации, которая существует при отказе функции безопасности ПСБ, выполняемой по запросу. Она зависит от того, существуют ли независимые способы предупреждения людей об опасности, прежде чем она возникнет, и о путях эвакуации
Интенсивность запросов	W	Количество случаев в год, когда опасное событие происходит при отсутствии рассматриваемой функции безопасности ПСБ. Его можно определить, рассмотрев все отказы, приводящие к опасному событию, и оценив общую частоту происшествий. Другие СЗ также должны учитываться

D.3 Калибровка

Процесс калибровки преследует следующие цели:

a) описать все параметры таким образом, чтобы дать возможность команде, занимающейся оценкой УПБ, сделать объективное заключение, основанное на характеристиках объекта;

b) обеспечить соответствие выбранного для данного объекта УПБ корпоративному критерию риска и обеспечить при определении УПБ учет возможного риска со стороны других источников;

c) обеспечить проверку процесса выбора параметров.

Калибровка графа риска — это процесс присвоения численных значений параметрам графа риска. При этом формируется базис для оценки существующего риска процесса и оказывается возможным определить требуемую полноту безопасности рассматриваемой функции безопасности ПСБ. Каждому параметру присваивается диапазон значений, таких, что, будучи примененными в комбинации, они позволяют получить количественную оценку риска, существующего в отсутствие данной функции безопасности. Так устанавливается мера степени доверия функции безопасности ПСБ. Граф риска связывает определенные комбинации параметров риска с УПБ. Связь между комбинациями параметров риска и УПБ устанавливается путем рассмотрения величины допустимого риска, связанного с конкретной опасностью.

Рассматривая калибровку графа риска, важно принять во внимание требования к риску, возникающие как со стороны собственников, так и со стороны регламентирующих органов. Риск для жизни может быть рассмотрен с двух позиций:

- индивидуальный риск — определяется как риск в течение года для лиц, наиболее подверженных риску. Обычно задается максимально допустимое его значение, которое обычно учитывает совокупность воздействий от всех источников опасности;
- общественный риск — определяется как общий риск в течение года, испытываемый группой лиц. Обычное требование в этом случае состоит в том, чтобы снизить общественный риск, по меньшей мере, до такого значения, которое может быть воспринято обществом как допустимое и дальнейшее снижение которого связано с непропорциональными по отношению к результату затратами.

Если необходимо снизить индивидуальный риск до определенного максимально допустимого уровня, то нельзя полагать, что такое снижение риска может быть достигнуто применением какой-либо одной ПСБ. Лицо, подвергаемое риску, может находиться под воздействием многих его источников (например, риски падения, пожара, взрыва).

При рассмотрении требуемой степени снижения риска организация может исходить из критериев, связанных с приращением стоимости устранения фатального исхода. Эту величину можно подсчитать, разделив суммированные за год расходы на дополнительное оборудование и технику, обеспечивающие увеличение полноты безопасности, на приращение сокращения риска. Дополнительный УПБ считается оправданным, если приращение затрат на устранение фатального исхода оказывается меньше предусмотренного ранее значения.

Широко применяемый критерий для общественного риска базируется на вероятности F появления N фатальных исходов. Критерий допустимого общественного риска имеет вид кривой или семейства кривых в логарифмической шкале, связывающих число фатальных исходов с частотой несчастных случаев. Проверка соблюдения требований к общественному риску выполняется путем построения кривой, отражающей зависимость накопленной частоты возникновения несчастных случаев от их последствий (график F — N). Далее следует убедиться, что эта кривая не пересекает кривую допустимого риска.

Все эти соображения следует принять во внимание перед тем, как установить значения каждого из параметров. Большинству параметров присваивается определенный диапазон (например, если ожидаемая частота запроса оказывается в пределах определенного уровня значений запросов в год, то можно использовать параметр W3). Аналогично в случае запросов, имеющих частоту ниже на порядок, применяется параметр W2, а на следующем, еще более низком уровне — параметр W1. Присвоение каждому параметру определенного уровня помогает команде специалистов принять решение о том, какое значение параметра выбрать для конкретного объекта. Для калибровки графа риска каждому параметру присваивается или численное значение, или определенный диапазон. Риск,

связанный с каждой из комбинаций параметров, далее оценивается с позиций индивидуального и социального рисков. Затем можно определить величину снижения риска, удовлетворяющую требованиям (риск должен быть равен или меньше допустимого). С помощью этого метода для каждой комбинации параметров может быть определен уровень полноты безопасности. Нет необходимости проводить эту работу по калибровке каждый раз, когда требуется определить УПБ для конкретного случая. Как правило, бывает достаточно провести эту работу однократно для каждой опасности. Если исходные предположения, принятые при калибровке, оказываются неверными для конкретного проекта, то могут потребоваться уточнения.

Если оценки параметров выполнены, то необходимо располагать информацией о том, как эти оценки были получены.

Важно, чтобы этот процесс калибровки был согласован в организации на верхнем уровне, отвечающем за безопасность. Принятые решения определяют общий достигнутый уровень безопасности.

В общем случае с помощью графа риска сложно определить возможность зависимого отказа между источниками запроса и ПСБ. При этом может потребоваться провести переоценку эффективности ПСБ.

D.4 Организация и состав команды специалистов для определения УПБ

Маловероятно, чтобы отдельный специалист обладал необходимым умением и опытом для принятия самостоятельного решения относительно всех соответствующих параметров. Для этого обычно используют командный подход, причем задача команды — определить УПБ. В состав такой команды, как правило, входят:

- специалист по технологическому процессу;
- инженер — специалист по управлению процессом;
- инженер по эксплуатации;
- специалист по безопасности;
- специалист, имеющий практический опыт эксплуатации рассматриваемого процесса.

Команда обычно рассматривает поочередно каждую функцию безопасности ПСБ. При этом команде требуется иметь подробную информацию о процессе и вероятном числе лиц, подвергающихся риску.

D.5 Оформление документов по результатам определения УПБ

Очень важно, чтобы все решения, принимаемые в процессе определения УПБ, были зафиксированы в документах, связанных с управлением конфигурацией. Из документации должно быть ясно, почему командой были выбраны данные конкретные параметры, связанные с функцией безопасности. Заполненные формы принятых предположений и основанных на них результатах определения УПБ каждой функции безопасности должны быть скомплектованы в досье. Если установлено, что в области, обслуживаемой одной командой, имеется целый ряд систем, выполняющих функции безопасности, то может оказаться необходимым пересмотреть правомерность допущений, принятых при калибровке. В досье следует также включать следующую дополнительную информацию:

- граф риска с описанием всех диапазонов параметров;
- номера всех используемых проектных и измененных документов;
- ссылки на известные допущения и результаты любых исследований, которые были использованы при оценке параметров;
- ссылки на отказы, которые приводили к запросам, и на ошибочные модели развития события, в которых эти отказы были использованы для определения частоты запросов;
- ссылки на источники данных, использованных при определении интенсивности запросов.

D.6 Пример калибровки, основанной на типовом критерии

Таблица D.2, в которой даны описания параметров и диапазоны каждого из них, была составлена в соответствии с конкретным критерием, типичным для химических процессов, по процедуре, рассмотренной выше. Прежде чем использовать эту таблицу в контексте любого проекта, важно подтвердить, что она отвечает требованиям тех лиц, которые несут ответственность за безопасность.

Для модификации параметра, характеризующего последствия, введена концепция степени защищенности, поскольку во многих случаях отказ не приводит к немедленному фатальному исходу. Уязвимость лица, подвергающегося опасности, — это важный аспект анализа риска, поскольку, например, доза опасного воздействия, полученная человеком, может оказаться недостаточной для того, чтобы вызвать фатальный исход. Уязвимость по отношению к последствиям опасного события есть функция концентрации опасности, которой подвергся человек, и длительности воздействия этой опасности. Пусть, например, отказ приводит к повышению давления в сосуде, но не выше, чем испытательное давление. Обычно подобный отказ может привести к утечке через фланец. В этом случае события, скорее всего, будут развиваться достаточно медленно и у обслуживающего персонала будет возможность избежать последствий. Даже в случае большой утечки жидких компонентов эскалация опасности будет достаточно медленной, и оперативному персоналу с большой вероятностью удастся избежать опасности. Конечно, встречаются случаи, в которых отказ может приводить к разрыву трубопровода или стенки сосуда; в таких случаях уязвимость персонала может быть высокой.

Анализ признаков развития опасного события может привести к увеличению количества людей, находящихся в опасности. Всегда следует рассмотреть наихудший сценарий развития событий.

Важно осознать разницу между «уязвимостью» (У) и «вероятностью того, что опасности можно избежать» (Р), что позволит не учитывать дважды один и тот же фактор. Уязвимость — это мера, которая связана со скоростью развития событий после возникновения опасности, в то время как параметр Р — это мера, связанная с предотвращением опасности. Параметр P_A следует применять только в тех случаях, когда опасность может быть предотвращена в результате действий оператора, после того как он придет к выводу, что ПСБ отказала.

Существуют некоторые ограничения на выбор параметров обитаемости. Требуется выбрать фактор заселенности по наименее защищенному лицу, а не по среднему для всех лиц. Обоснованием этому является стремление обеспечить, чтобы ни такое лицо, ни тем более остальные люди не подвергались высокому риску.

Если параметр не попадает ни в какой из характерных диапазонов, то требования к снижению риска следует установить каким-либо иным методом или провести повторную калибровку графа риска, используя описанные выше методы.

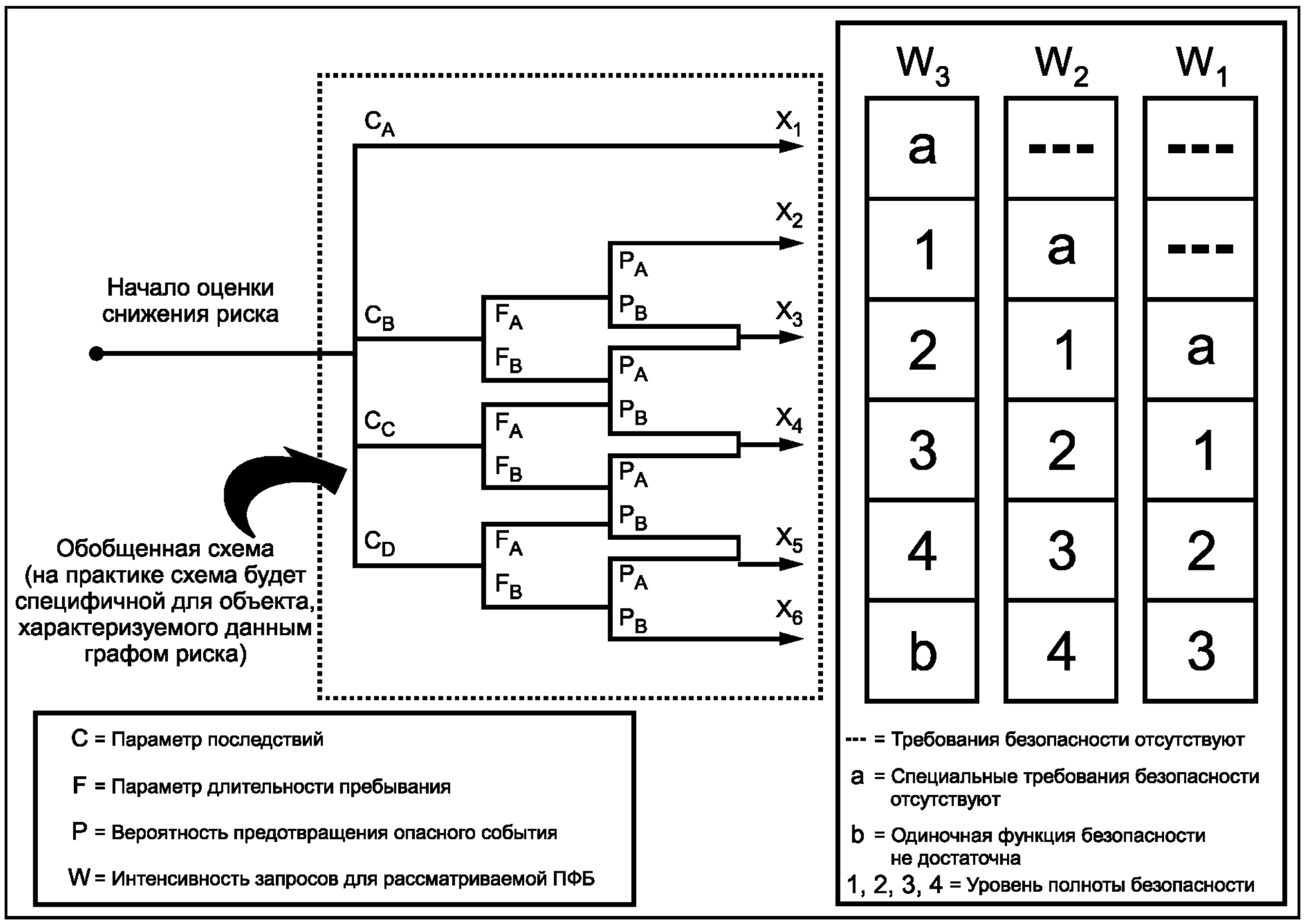


Рисунок D.1 — Граф риска, общая схема

Таблица D.2 — Пример калибровки графа риска общего назначения

Параметр риска		Классификация	Комментарии
Последствия (С). Число фатальных исходов. Подсчитывается умножением числа людей, находящихся в опасной области, на уязвимость к определенной опасности. Уязвимость определяется природой опасности, от которой осуществляется защита. Могут использоваться следующие факторы: V = 0,01 Небольшой выброс воспламеняющихся или токсичных материалов. V = 0,1 Большой выброс воспламеняющихся или токсичных материалов.	C_A C_B C_C C_D	Минимальный ущерб Диапазон 0,01—0,1 Диапазон > 0,1—1,0 Диапазон > 1,0	1 Система классификации относится к случаям фатального исхода или травм для людей. 2 При интерпретации параметров C_A, C_B, C_C и C_D следует принимать во внимание последствия несчастного случая и нормальное их устранение

Окончание таблицы D.2

Параметр риска		Классификация	Комментарии
V = 0,5 То же, что и выше, но велика вероятность возгорания либо высокотоксичный материал. V = 1 Разрушение или взрыв			
Заселенность (F) Определяется как доля времени пребывания людей в области, подвергающейся опасности, по отношению к величине периода работы Примечания 1 Если время пребывания в опасной области различно для различных смен, то следует выбирать наибольшее время. 2 Величину F_A следует применять только в тех случаях, когда частота запроса случайна и не зависит от того, превышает ли обитаемость обычное значение. Последнее характерно для случаев, когда запросы возникают при пуске оборудования или во время изучения ненормальных ситуаций.	F_A F_B	От редкого до более частого нахождения в опасной области. Обитаемость меньше чем 0,1. От частого до постоянного пребывания в опасной области	3 См. выше комментарий 1
Вероятность избежать опасного события (P), если отказывает система защиты	P_A P_B	Принимается, если выполняются условия графы 4. Принимается, если условия не выполняются	4 P_A следует выбирать, только если справедливы следующие условия: - предусмотрены средства оповещения оператора об отказе ПСБ; - предусмотрены независимые средства останова процесса так, чтобы избежать опасности или позволить персоналу эвакуироваться в безопасную зону; - время между оповещением оператора и опасным событием превышает 1 час или явно достаточно для выполнения необходимых действий
Интенсивность запросов (W). Количество случаев в год, когда опасное событие возникает при отсутствии ПСБ. Для того чтобы определить частоту запроса, необходимо рассмотреть все причины отказа, которые могут привести к возникновению одного и того же опасного события. При определении интенсивности запросов роль системы управления и ее вмешательство в ход процесса следует учитывать в минимальной степени. Если система спроектирована и эксплуатируется не в соответствии с МЭК 61511, то ее функционирование ограничено уровнем безопасности ниже, чем УПБ1	W_1 W_2 W_3	Частота запросов меньше чем 0,1 *D* в год. Частота запросов лежит в диапазоне 0,1 *D* и *D* в год. Частота запросов лежит в диапазоне между *D* и 10 *D*. При частотах запросов, больших чем 10 *D*, потребуется более высокий уровень полноты безопасности	5 Цель введения фактора W — оценить частоту появления опасности без ПСБ. Если частота запроса очень велика, то УПБ следует определять либо другим методом, либо путем перекалибровки графа риска. Следует отметить, что методы графа риска могут оказаться не лучшим решением задачи, если объект работает в непрерывном режиме (см. МЭК 61511-1, пункт 3.2.43.2). 6 C является градуировочным коэффициентом, значение которого следует определять исходя из корпоративного критерия допустимого риска с учетом других источников риска для людей, ему подвергающихся
Примечание — Этот пример предназначен для иллюстрации принципов построения графов риска. Граф риска для конкретного приложения и конкретных опасных ситуаций должен быть согласован с условиями, учитываемыми при определении допустимого риска (см. D.1—D.6).			

D.7 Применение графа риска, когда последствия — это причинение вреда окружающей среде

Подход, использующий граф риска, может быть также применен для определения требований УПБ, когда последствия отказа включают причинение серьезного вреда окружающей среде. Необходимый УПБ зависит от характеристик субстанции, попадающей в окружающую среду, и от чувствительности последней. Ниже приведена общая таблица, в которой последствия опасного события сформулированы в терминах окружающей среды. На каждом отдельно размещенном предприятии может быть использовано некое вещество, о наличии которого следует уведомить местные власти. Уже на стадии проектирования следует установить, что может быть приемлемым для конкретного местоположения.

Таблица D.3 — Общие последствия для окружающей среды

Параметр риска		Классификация	Комментарии
Последствия (C)	C_A	Выброс, причинивший не очень серьезный вред, но такой, что об этом необходимо доложить местной администрации.	Умеренный выброс из фланца или клапана. Незначительный разлив жидкости. Небольшое загрязнение земли, не влияющее на подземные воды.
	C_B	Выброс в пределах ограждения (предприятия, объекта) с причинением значительного вреда.	Облако вредных газов над установкой как следствие выброса из фланца или отказа уплотнения в компрессоре.
	C_C	Выброс за ограждение с причинением существенного вреда, однако последствия могут быть быстро ликвидированы без значительных длительных последствий.	Выброс пара или аэрозоля с одновременным выбросом жидкости (или без него), причинивший длительный ущерб растениям и фауне.
	C_D	Выброс за ограждение с причинением существенного вреда, когда последствия не могут быть быстро ликвидированы или имеются значительные длительные последствия.	Сброс жидкости в реку или море. Выброс пара или аэрозоля с одновременным выбросом жидкости (или без него), причинивший длительный ущерб растениям и фауне. Выброс твердых веществ (пыли, катализатора, золы). Выброс жидкости с попаданием в подземные воды.

Описанные выше последствия опасного события могут быть использованы для анализа совместно со специальной формой графа риска, которая приведена ниже (рисунок D.2). Следует отметить, что в этой версии графа риска не используется параметр F, поскольку в этом случае понятие заселенности не применяют. Остальные параметры P и W используют, и их определения могут быть идентичны тем, которые были применены выше.

D.8 Применение графа риска для случая имущественных потерь

Метод графа риска можно применить для определения требований к полноте безопасности и в том случае, когда последствия отказа включают потери имущества. Потери имущества — это общие экономические потери, связанные с отказом функционирования по запросу. Они включают потери на восстановление, если был причинен вред оборудованию, а также потерю испорченной или утраченной продукции. УПБ, соответствующий последствиям, связанным с такими потерями, может быть определен с помощью обыкновенного анализа стоимости. Если метод графа риска применяют для определения УПБ, связанных с последствиями опасного события для окружающей среды, то его целесообразно использовать и для случая имущественного ущерба. При этом требуется определить параметры C_A — C_D, которые могут изменяться в широких пределах для разных компаний.

Граф риска, аналогичный использованному для случая защиты окружающей среды, может быть сформирован и в случае имущественных потерь. Следует отметить, что в этой версии графа риска не используют параметр F, поскольку в этом случае понятие обитаемости не применяют. Остальные параметры P и W используют, и их определения могут быть идентичны тем, которые приведены выше.

D.9 Определение УПБ для функции безопасности ПСБ, когда последствия опасного события включают более одного типа потерь

Часто последствия отказа при выполнении действий по запросу связаны с несколькими категориями потерь. В таких случаях требования к УПБ, связанные с каждой из категорий потерь, следует определять отдельно. При этом для анализа каждого вида выявленного риска можно использовать различные методы. Если происходит отказ функции, выполняемой по запросу, УПБ, установленный для такой конкретной функции, должен учитывать кумулятивное воздействие всех выявленных рисков.

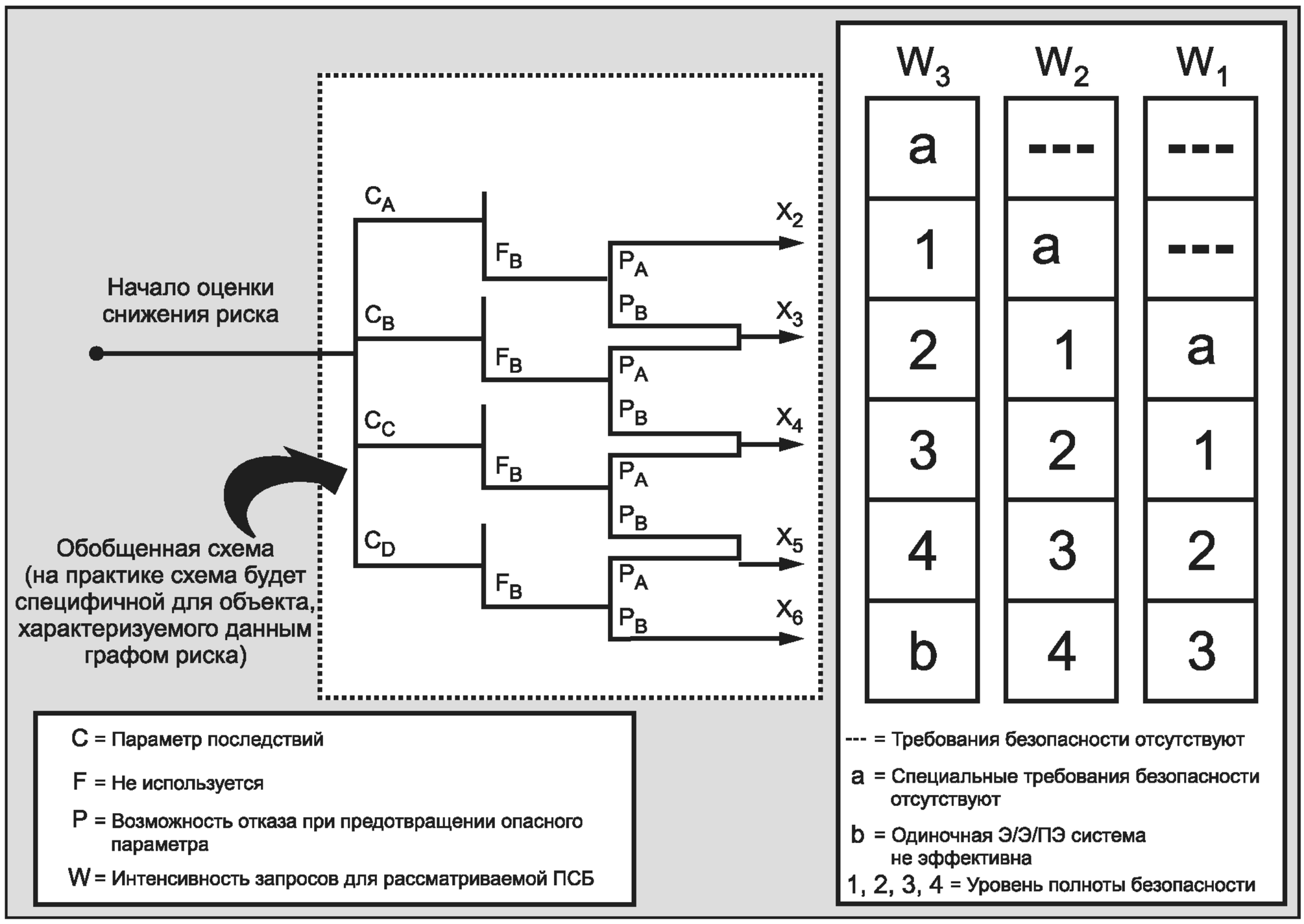


Рисунок D.2 — Граф риска: случай ущерба для окружающей среды

Приложение Е
(справочное)

Определение требуемых уровней полноты безопасности. Качественный метод. Граф риска

Е.1 Общие сведения

Данное приложение базируется на методах, более детально изложенных в [11].

В данном приложении описан метод графа риска для определения УПБ функций безопасности ПСБ. Это качественный метод, который позволяет определить УПБ функций безопасности ПСБ при известных факторах риска, связанных с процессом и с его основной системой управления процессом.

В предлагаемом подходе использован ряд параметров, которые совместно описывают природу опасной ситуации, возникающей в случае отказа или отсутствия приборной системы. В каждом из четырех наборов параметров выбирают по одному параметру. Комбинация выбранных параметров позволяет установить УПБ для функций безопасности ПСБ. Указанные параметры:

- позволяют получить ранжированную оценку уровней риска и
- представляют собой ключевые факторы оценки риска.

Подход, использующий граф риска, может быть также применен для определения необходимости снижения риска в тех случаях, когда последствия включают серьезный ущерб для окружающей среды или имущественные потери.

В данном приложении показано применение метода (подробно описанного в [12] и [13]) для технологических процессов и в машиностроении. Этот метод использовали много лет в машиностроении и технологических процессах в Германии. Метод был принят TÜV (Аккредитованная испытательная лаборатория Германии) и регулирующими органами Германии, ответственными за указанный сектор промышленности. Этот граф применяют для определения УПБ систем, связанных с безопасностью; связь между графом и УПБ показана на рисунках Е.1 и Е.2.

Е.2 Типовая реализация функции безопасности ПСБ

Существует четкое различие между общими задачами обеспечения безопасности объекта и эксплуатационными требованиями к безопасности процесса, достигаемой с помощью средств управления. В связи с этим применяется следующая классификация систем управления процессом:

- основная система управления процессом;
- система мониторинга процесса;
- приборная система безопасности.

Цель такой классификации — сформулировать требования к каждому типу систем, необходимые для выполнения общих требований предприятия при экономически разумных затратах. Эта классификация позволяет детально очертить круг вопросов, решаемых при планировании, сооружении и эксплуатации объекта, а также при его последующей модификации в части системы управления процессом.

ОСУП используются для обеспечения правильного функционирования процесса в нормальных условиях. Такая система реализует измерение, управление и/или запись всех соответствующих переменных процесса. ОСУП или действует в непрерывном режиме, или к ее действиям прибегают для вмешательства в ход процесса до того, как оказывается необходимой реакция ПСБ. (В ОСУП обычно нет необходимости соблюдать требования настоящего стандарта.)

Системы мониторинга процесса действуют при определенных условиях, когда одна или более из переменных процесса оказываются вне нормального диапазона изменения. Системы мониторинга выполняют предаварийную сигнализацию нарушений допустимого состояния процесса, чтобы привлечь внимание оперативного персонала или стимулировать вмешательство человека в работу объекта (система мониторинга обычно не нуждается в необходимости соблюдать требования настоящего стандарта).

ПСБ либо предотвращают опасное состояние объекта («система защиты»), либо уменьшают последствия опасного события.

Если ПСБ отсутствует, то возможно возникновение опасного события с травмами для персонала.

В отличие от функций ОСУП для функций ПСБ обычно характерна низкая частота запросов. Это происходит, прежде всего, потому, что вероятность опасного события низка. Кроме того, объект всегда оснащен ОСУП и системами мониторинга, которые способствуют снижению частоты запросов на срабатывание ПСБ.

Е.3 Синтез графа риска

Граф риска базируется на том принципе, что риск пропорционален частоте появления опасного события и размеру его последствий. Первоначально принимается, что ПСБ нет, зато присутствуют ОСУП и системы мониторинга, не являющиеся ПСБ.

Последствия связаны с причинением вреда здоровью и безопасностью или причинением вреда окружающей среде.

Частота появления опасных событий зависит от следующих факторов:

- частота и возможное время пребывания людей в опасной зоне;
- возможность избежать опасного события;
- вероятность того, что опасное событие возникает при отсутствии ПСБ (все остальные средства снижения внешнего риска предполагаются действующими), так называемая «вероятность нежелательного события».

Из сказанного следует, что существуют четыре параметра риска:

- последствие опасного события (C);
- частота пребывания в опасной зоне, умноженная на время воздействия опасных условий (F);
- возможность избежать последствий опасного события (P);
- вероятность нежелательного происшествия (W).

Если граф риска применяют для определения УПБ функции безопасности, выполняемой в непрерывном режиме, то необходимо рассмотреть изменения параметров, используемых в графе риска. Рекомендуется, чтобы параметры, представляющие факторы риска, наилучшим образом соответствовали характеристикам рассматриваемого применения. Необходимо также рассмотреть связь УПБ с решениями по выбору параметров, поскольку для обеспечения снижения риска до приемлемого уровня может понадобиться настройка. Например, параметр W может быть определен заново как процентное отношение времени активной работы системы безопасности к общему времени ее работы на объекте. При таком выборе W1 опасность не является непрерывно действующим фактором и период времени, в котором отказ будет приводить к появлению опасности, будет составлять малую долю года. В этом примере следует пересмотреть и другие параметры, чтобы соответствующие критерии принятия решения и пересмотренные результаты определения УПБ обеспечивали допустимый риск.

E.4 Реализация графа риска. Защита персонала

Граф риска, соответствующий описанной выше комбинации параметров, показан на рисунке E.1. Параметры с более высокими значениями индексов соответствуют более высокому риску ($C_1 < C_2 < C_3 < C_4$; $F_1 < F_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$). Классификация параметров, соответствующая рисунку E.1, приведена в таблице E.1. Граф применяют отдельно для каждой функции безопасности. Он позволяет определить требуемый для этой функции УПБ.

При определении риска, который должен быть предотвращен ПСБ, оценку риска следует проводить исходя из отсутствия на объекте рассматриваемой ПСБ. Основные исходные параметры такой оценки — это тип и масштабы развития воздействий, а также ожидаемая частота появления опасного состояния технологического процесса.

Риск может быть определен и проверен с помощью метода, детально изложенного в [12], который позволяет по установленным параметрам определить классы требований. Как правило, чем выше порядковый номер класса требований, тем большая часть риска снимается ПСБ и, следовательно, в общем случае более строгими являются требования и результирующие показатели.

Для промышленных технологических процессов требования классов АК7 и АК8 не могут быть обеспечены с помощью одних ПСБ. Чтобы добиться снижения риска, как минимум, до уровня требований класса АК6, требуются специальные средства управления, не связанные с процессом.

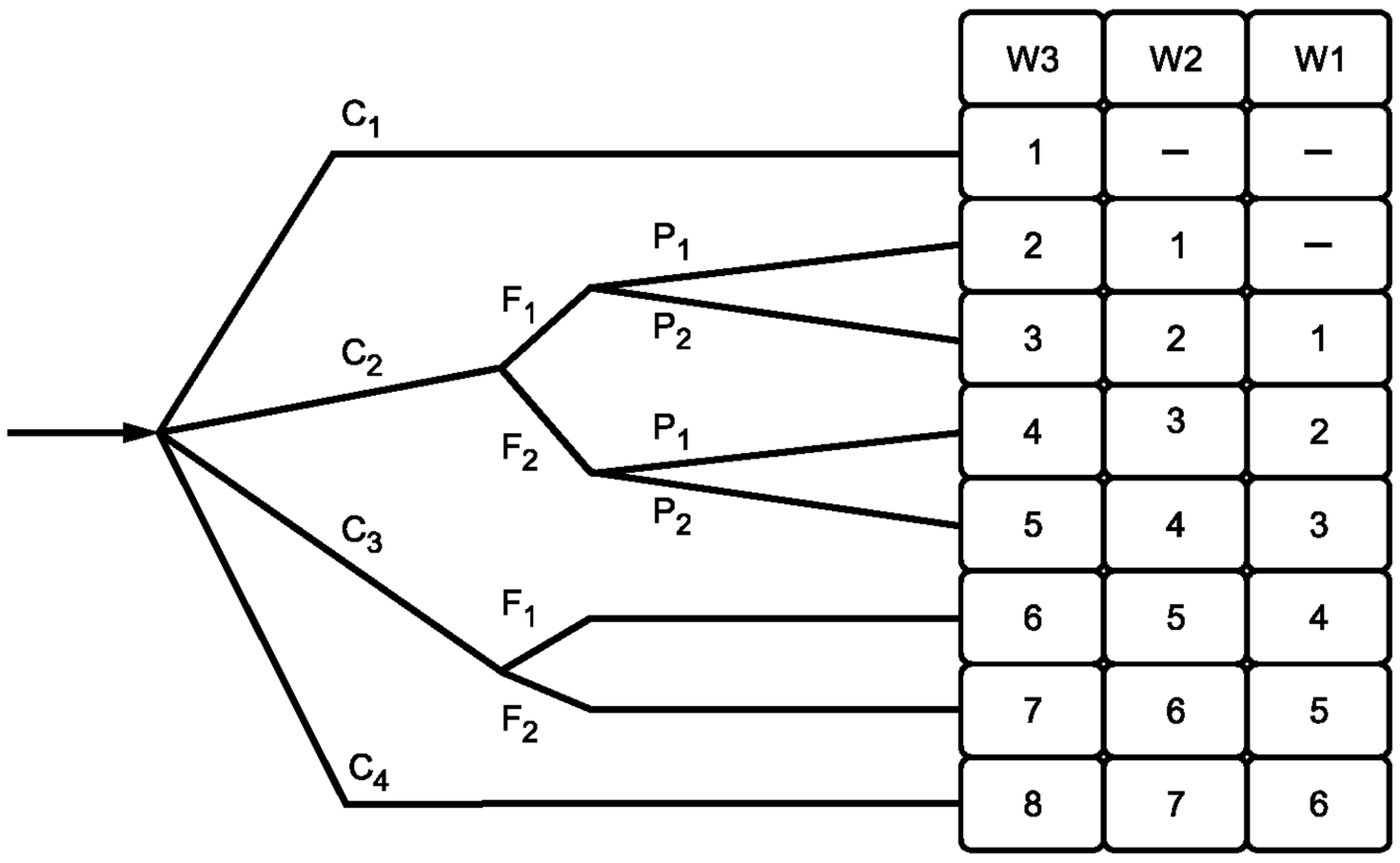


Рисунок E.1 — Граф риска по [12] — защита персонала (см. таблицу E.1)

Поскольку формулировать индивидуальные требования с соответствующими наборами показателей для каждого отдельного класса требований непрактично, то предлагается согласно [13] выполнить разделение риска на две области.

Область риска 1: более низкий риск (компенсируется при УПБ 1 и УПБ 2).

Область риска 2: более высокий риск (компенсируется при УПБ 3).

Соотношение между классами требований по [12] и областями риска показано на рисунке Е.2.

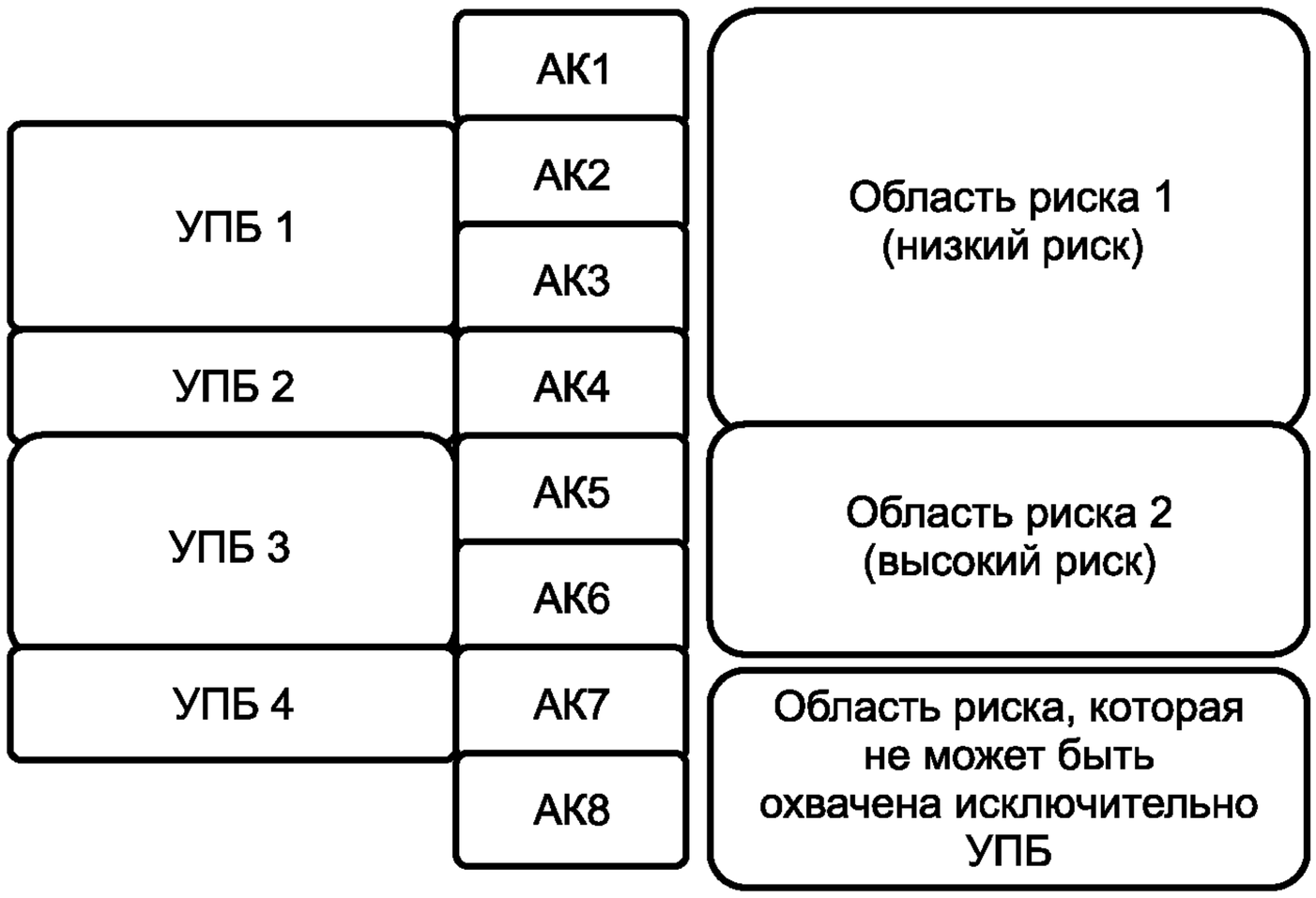


Рисунок Е.2 — Соотношение между стандартами серии МЭК 61511, [12] и [13]

Е.5 Вопросы, которые следует рассмотреть при применении графов риска

Применяя метод графа риска, очень важно рассмотреть требования, предъявляемые собственником и регламентирующими органами.

Интерпретацию и оценку каждой ветви графа риска следует описывать и документально оформлять в ясных и понятных терминах для обеспечения последовательности использования метода.

Очень важно, чтобы граф риска был согласован с руководством компании, отвечающей за безопасность.

Таблица Е.1 — Данные, относящиеся к графу риска

Параметр риска		Классификация	Комментарии
Последствия (С)	C_1	Легкие травмы у персонала	1 Эта система классификации отражает события, связанные с травмами или смертью людей. Для случаев ущерба окружающей среде и имуществу потребуются другие системы классификации
	C_2	Серьезные травмы у одного или более человек. Один смертельный исход	
	C_3	Смерть нескольких человек	
	C_4	Катастрофические последствия, многочисленные жертвы	
Частота фактов пребывания в опасной области, умноженная на время пребывания (F)	F_1	От редкого до более частого пребывания в опасной зоне	2 См. выше комментарий 1
	F_2	От частого до постоянного пребывания в опасной зоне	

Окончание таблицы Е.1

Параметр риска		Классификация	Комментарии
Возможность избежать последствий опасного события (Р)	P_1	Возможно при некоторых условиях	3 Этот параметр учитывает следующее: - Управление процессом (контролируемое, т. е. выполняемое квалифицированными или неквалифицированными лицами, или неконтролируемое); - темп развития опасного события (например, внезапно, быстро или медленно); - легкость распознавания опасности (например, видна непосредственно, распознается с помощью или без помощи технических средств); - возможность избежать последствий опасного события (например, эвакуация возможна, невозможна или возможна при определенных обстоятельствах); - наличие фактического опыта в области безопасности (такой опыт мог быть приобретен на аналогичных или подобных объектах)
	P_2	Почти невозможно	
Возможность возникновения нежелательного события (W)	W_1	Очень малая вероятность появления нежелательных событий. Возможно лишь редкое их появление	4 Назначение фактора W — оценить частоту появления нежелательных событий при отсутствии приборной системы безопасности (Э/Э/ПЭ или иные технологии), но при применении каких-либо внешних средств снижения риска
	W_2	Малая вероятность появления нежелательных событий. Возможно лишь редкое их появление	
	W_3	Относительно высокая вероятность появления нежелательных событий. Возможно частое их появление	

Приложение F
(справочное)

Анализ слоев защиты

F.1 Введение

В данном приложении описан метод, получивший название «Анализ слоев защиты» (АСЗ). Исходными данными для применения этого метода являются результаты анализа, полученные методом HAZOP. Далее учитывают каждую выявленную опасность путем документального оформления всех вызвавших ее причин. Кроме этого, учитывают все слои защиты, которые предотвращают либо ослабляют эту опасность. По этим данным определяют общую меру снижения риска и анализируют необходимость дальнейшего его снижения. Если необходимо дальнейшее снижение риска и его предполагается проводить путем введения функции безопасности ПСБ, то метод АСЗ позволяет определить соответствующий этой функции УПБ.

Данное приложение не содержит подробного описания метода, а предназначено для иллюстрации общих принципов его применения. Более подробно метод описан в [8].

F.2 Анализ слоев защиты

Анализ жизненного цикла безопасности, определенный в МЭК 61511-1, требует определения УПБ при создании функции безопасности ПСБ. Метод АСЗ, описываемый ниже, позволяет группе, состоящей из специалистов разного профиля, определить УПБ для функций безопасности ПСБ на действующем объекте. В состав группы должны входить следующие специалисты:

- оператор, имеющий опыт работы на рассматриваемом процессе;
- инженер — эксперт по данному процессу;
- технолог;
- инженер — специалист в области управления процессами;
- специалист по техническому обслуживанию аппаратуры (в том числе электрической), имеющий опыт эксплуатации данного процесса;
- специалист в области анализа риска.

Один из участников группы должен быть обучен применению метода АСЗ.

Информация, требующаяся для применения метода АСЗ, содержится в данных, собранных и полученных в результате применения анализа опасности и работоспособности (HAZOP). Связь между данными, требующимися для применения АСЗ, и данными, полученными методом HAZOP, показана в таблице F.1. На рисунке F.1 показана типичная форма, которую можно использовать при применении метода АСЗ.

Метод АСЗ, анализируя опасные события, позволяет определить, требуются ли на данном процессе функции безопасности ПСБ, и если требуются, то позволяет для каждой из таких функций определить УПБ.

F.3 Влияющее событие

Пользуясь бланком, приведенным на рисунке F.1, описание (последствие) каждого влияющего события, полученное методом HAZOP, заносят в графу 1.

F.4 Уровень тяжести события

Далее согласно таблице F.2 выбирают уровни тяжести влияющего события: малый (M), серьезный (S) или высокий (E) — и заносят в графу 2 на рисунке F.1.

Таблица F.1 — Данные, которые HAZOP готовит для АСЗ

Требования АСЗ	Данные, выявленные HAZOP
Информация	Информация
Опасное событие	Последствия
Уровень тяжести опасного события	Тяжесть последствий
Исходная причина	Причина
Вероятность появления исходной причины	Частота возникновения причин
Слои защиты	Используемые средства защиты
Требуемое дополнительное ослабление	Рекомендуемые новые средства защиты

F.5 Исходные причины

Все причины, инициирующие появление опасного события, записывают в графу 3 на рисунке F.1. Опасное событие может иметь много исходных причин, и важно перечислить их все.

№	1	2	3	4	5			6	7	8	9	10	11
					СЛОИ ЗАЩИТЫ								
	Описание влияющего события, F.3, F.14.1	Уровень тяжести влияющего события, F.4, F.14.1	Исходная причина, F.5, F.14.2	Вероятность появления исходной причины, F.6, F.14.3	Общее проектирование процесса, F.14.4	ОСУП, F.14.5	Сигнализация и т. п., F.14.6	Дополнительное ослабление, ограничение доступа, F.8, F.14.7	Дополнительные НСЗ, предохранительные клапаны, F.9, F.14.8	Вероятность промежуточного события, F.10, F.14.9	УПБ функции безопасности ПСБ, F.11, F.14.10	Вероятность ослабления влияющего события, F.12, F.14.10	Примечание
1	Пожар из-за разрушения колонны	S	Отсутствие охлаждающей воды	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	Высокое давление вызывает разрушение колонны
2	Пожар из-за разрушения колонны	S	Отказ контура управления паром	0,1	0,1		0,1	0,1	PRV 01	10^{-6}	10^{-2}	10^{-8}	То же
№													

Примечание — Уровни тяжести события: E — высокий, S — серьезный, M — малый. Возможность характеризуется числом событий в год. Другие численные данные являются средними вероятностями при наличии запроса.

Рисунок F.1 — Отчет по АСЗ

Таблица F.2 — Уровни тяжести влияющего события

Уровень тяжести	Последствия
Малый уровень (M)	Воздействие, первоначально ограниченное локальной зоной появления события с тенденцией к расширению последствий при отсутствии корректирующих действий
Серьезный уровень (S)	Опасное событие может привести к тяжелым травмам или к фатальному исходу как в локальной зоне, так и вне ее
Высокий уровень (E)	Опасное событие, в пять или более раз более жесткое, чем серьезное событие

F.6 Вероятность появления исходных причин

Численное значение вероятности появления исходных причин, измеряемое числом событий в год, заносят в графу 4 рисунка F.1. Типичные значения вероятности появления (*f*) таких причин приведены в таблице F.3. Для определения вероятности исходной причины очень важен опыт упоминавшейся группы специалистов.

Т а б л и ц а F.3 — Вероятность появления исходных причин

Низкая	Отказ или серия отказов с очень низкой вероятностью появления в течение ожидаемого жизненного цикла объекта, например: - три или более одновременных отказов приборов или ошибок оператора; - самопроизвольный отказ отдельного резервуара или иного оборудования процесса	$f < 10^{-4}$ *в год*
Средняя	Отказ или серия отказов с низкой вероятностью появления в течение ожидаемого жизненного цикла объекта, например: - отказы резервированного прибора или клапана; - комбинация отказов приборов и ошибок оператора; - единичный отказ небольшой технологической линии или фитинга	$10^{-4} < f < 10^{-2}$ *в год*
Высокая	Отказы, которых следует ожидать в течение жизненного цикла объекта, например: - утечки в процессе; - одиночные отказы прибора или клапана; - ошибки человека, способные привести к выбросам материала	$10^{-2} < f$ *в год*

F.7 Слои защиты

На рисунке 2 показаны многочисленные слои защиты, которые обычно применяют для промышленных процессов. Каждый слой защиты представляет собой совокупность технических средств и/или административных мер, которые функционируют совместно с другими слоями защиты. Слои защиты, которые выполняют свои функции с высокой степенью надежности, могут считаться независимыми слоями защиты (НСЗ) (см. F.9).

Проектные решения, направленные на уменьшение возможности появления исходных событий, приведены в графе 5 на рисунке F.1. Примером может служить использование защитной рубашки для трубопровода или емкости. Такая рубашка должна предотвращать выброс материала в случае разрушения.

В следующей колонке графы 5 на рисунке F.1 приведена информация, связанная с ОСУП. Если контур управления, реализуемый ОСУП, предотвращает появление опасного события при возникновении исходных причин, то его влияние характеризуют сокращением средней частоты отказов при наличии запроса.

В последней колонке графы 5 на рисунке F.1 указывается влияние аварийной сигнализации, которая привлекает внимание оператора и стимулирует его вмешательство в процесс. Характерные величины средней частоты отказов при наличии запросов для уровней защиты приведены в таблице F.4.

Т а б л и ц а F.4 — Типичные значения вероятности отказа при запросе для слоев защиты (предотвращение и ослабление)

Слой защиты	Вероятность отказа при запросе
Контур управления	$1{,}0 \times 10^{-1}$
Работа оператора (опытного и в отсутствие стресса)	$1{,}0 \times 10^{-2}$ до $1{,}0 \times 10^{-5}$
Работа оператора в условиях стресса	0,5 до 1,0
Реакция оператора на аварийную сигнализацию	$1{,}0 \times 10^{-1}$
Давление внутри сосуда превышает максимально возможное, вызываемое внутренними и внешними причинами	10^{-4} или меньше, если сохраняется целостность емкости (т. е. коррозия под контролем, инспекцию и обслуживание проводят согласно расписанию)

F.8 Дополнительное ослабление

Ослабляющие слои относят к одной из трех категорий — механические, структурные и процедурные. Примерами могут служить:

- сброс давления;
- ограждения;
- ограниченный доступ.

Ослабляющие слои могут уменьшить тяжесть нежелательного события, но не предотвращают его появления. Примерами могут служить:

- система пожаротушения при появлении огня или дыма;
- пожарная сигнализация;
- меры по эвакуации персонала.

Группа специалистов, занимающаяся АСЗ, должна определить величины частоты отказов при запросах для всех ослабляющих слоев защиты и перечислить их в графе 6 на рисунке F.1.

F.9 Независимые слои защиты

НСЗ заносят в графу 7 на рисунке F.1.

Для того чтобы слой защиты считался независимым, он должен удовлетворять следующим критериям:

- защита должна обеспечивать значительное (минимум в сто раз) снижение определенного риска;
- функция защиты должна выполняться с высокой степенью готовности (0,9 и более);
- слой защиты должен обладать следующими важными характеристиками:

a) специфичность — НСЗ проектируется специально для того, чтобы предотвратить или ослабить последствия конкретной потенциально опасной ситуации (например, неуправляемая реакция, выброс токсичного материала, разгерметизация аппарата, пожар). Причин возникновения этой опасной ситуации может быть много, и, следовательно, действие НСЗ может происходить по многим сценариям, вызванным многочисленными исходными событиями;

b) независимость — НСЗ не зависит от других слоев защиты, связанных с той же выявленной опасностью;

c) надежность — можно рассчитывать, что НСЗ будет выполнять предназначенные для него функции, если при его проектировании учитывают как случайные, так и систематические отказы;

d) проверяемость — НСЗ должен облегчать проведение регулярного подтверждения соответствия функций защиты. При этом необходимы проверочные испытания и обслуживание системы безопасности.

Только такие слои защиты, которые пройдут испытания на соответствие требованиям работоспособности, специфичности, независимости, надежности и проверяемости, могут быть рассмотрены как независимые.

F.10 Вероятность возникновения промежуточного события

Вероятность возникновения промежуточного события подсчитывают умножением вероятности появления исходной причины (графа 4 на рисунке F.1) на значение вероятности отказа при наличии запроса для слоев защиты и ослабления (графы 5, 6 и 7 на рисунке F.1). Найденное значение имеет размерность числа событий в год, его заносят в графу 8 на рисунке F.1.

Если вероятность промежуточного события меньше, чем корпоративный критерий для событий этого уровня тяжести, то дополнительные слои защиты не требуются. Дальнейшее снижение риска следует проводить с учетом экономической целесообразности.

Если вероятность промежуточного события больше, чем корпоративный критерий для событий этого уровня тяжести, то требуется дальнейшее снижение риска. Перед тем как решить вопрос о введении дополнительного слоя защиты в виде ПСБ, следует рассмотреть возможность использования методов и решений, обеспечивающих большую безопасность. При этом данные на рисунке F.1 обновляют, производят пересчет вероятности появления промежуточного события и сравнение найденного значения с корпоративным критерием.

Если величину вероятности возникновения промежуточного события не удается сделать меньшей, чем корпоративный критерий, то требуется применить ПСБ.

F.11 Уровень полноты функции безопасности ПСБ

Если оказывается необходимым ввести новую функцию безопасности ПСБ, то следует подсчитать требуемый уровень ее полноты. Для этого величину корпоративного критерия для заданного уровня тяжести события нужно разделить на величину возможности появления промежуточного события. Среднее значение вероятности отказа (ВОНЗ$_{ср}$) при наличии запроса для функции безопасности ПСБ, лежащее ниже найденного в результате деления значения, принимают как максимальное для ПСБ и заносят в графу 9 на рисунке F.1.

F.12 Вероятность ослабления влияющего события

Далее подсчитывают значение вероятности ослабления влияющего события. Для этого значения граф 8 и 9 на рисунке F.1 перемножают и результат вносят в графу 10 на рисунке F.1. Эту процедуру продолжают до тех пор, пока группа специалистов не рассчитает вероятности ослабления событий для всех обнаруженных влияющих событий.

F.13 Полный риск

В качестве заключительного шага следует сложить вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, вызванными одной и той же опасностью. Например, вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, вызванных пожаром, сложить и использовать в формуле вида:

риск фатального исхода при пожаре = (общая вероятность ослабления влияющих событий, связанных с выбросом воспламеняющегося материала) × (вероятность возгорания) × (вероятность пребывания людей в опасной зоне) × (вероятность фатального исхода при пожаре).

Далее следует сложить вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, связанных с выбросом токсичных материалов, и использовать в аналогичной формуле:

риск фатального исхода при выбросе токсичных материалов = (общая вероятность ослабления влияющих событий, связанных с токсичными выбросами) × (вероятность пребывания людей в опасной зоне) × (вероятность фатального исхода вследствие токсичного выброса).

Экспертная оценка специалиста по анализу рисков и знания группы специалистов играют важную роль в уточнении и адаптации перечисленных выше показателей в формулах к условиям и практике работы объекта, а также к обществу, подвергаемому опасности.

Теперь можно определить полный риск для корпорации, связанный с данным процессом. Для этого следует объединить результаты, полученные расчетным путем по приведенным выше формулам.

Если полученное значение соответствует корпоративному критерию для персонала, подвергающегося опасности, или меньше его, то АСЗ можно считать завершенным. Однако поскольку персонал может подвергаться риску также со стороны других установок и проектов, то представляется разумным провести дальнейшее ослабление и снижение риска, если это окажется экономически оправданным.

F.14 Пример

Ниже приведен пример применения методологии АСЗ по отношению к опасному событию, выявленному методом HAZOP.

F.14.1 Влияющее событие и уровень его тяжести

Пусть с помощью метода HAZOP выявлено, что отклонение высокого давления в реакторе полимеризации периодического действия является опасным событием. Реактор из нержавеющей стали соединен последовательно с насадочной колонной из пластмассы, армированной стальной нитью и конденсатором, выполненным из нержавеющей стали. Трещина в армированной насадочной пластмассовой колонне может привести к выбросу воспламеняющегося газа, что, в свою очередь, может вызвать пожар при наличии источника воспламенения. Группа специалистов, пользуясь таблицей F.2, установила, что событие относится к уровню тяжести S (серьезный), поскольку оно может привести к серьезным травмам и даже фатальному исходу в опасной зоне. Влияющее событие и его тяжесть вносят соответственно в графы 1 и 2 на рисунке F.1.

F.14.2 Исходные причины

Методом HAZOP были зафиксированы две исходные причины повышения давления: прекращение подачи охлаждающей воды в конденсатор и отказ контура управления паром в реакторе. Обе эти причины внесены в графу 3 на рисунке F.1.

F.14.3 Вероятность исходных событий

Прекращение подачи охлаждающей воды на данном предприятии происходит, как показывает практика, один раз в 15 лет. Группа исследователей в качестве консервативной оценки приняла, что прекращение подачи охлаждающей воды происходит один раз в 10 лет. В графу 4 на рисунке F.1 вносят значение 0,1 события в год. Представляется разумным проследить до конца влияние этой причины и лишь затем обратиться к другой причине — к отказу контура управления паром в реакторе.

F.14.4 Проектирование слоев защиты

Зона процесса была спроектирована в соответствии с принятой классификацией применения электрического оборудования во взрывозащищенных зонах, и для нее реализован план управления безопасностью. Одним из элементов этого плана является управление процедурой замены электрического оборудования. По оценке группы АСЗ, риск воспламенения снижается в 10 раз благодаря управлению процедурами замены. Следовательно, влияние этого фактора равно 0,1. Это значение вносят в колонку «Общее проектирование процесса» графы 5 на рисунке F.1.

F.14.5 ОСУП

Высокое давление в реакторе сопровождается высокой температурой. В ОСУП предусмотрен контур управления, который изменяет подачу пара в рубашку реактора в зависимости от температуры в реакторе. Если температура в реакторе превышает заданное значение, то ОСУП прекратит подачу пара в рубашку реактора. Так как прекращение подачи пара способно предотвратить высокое давление, то ОСУП является слоем защиты. ОСУП является очень надежной цифровой системой управления, и оперативный персонал никогда не наблюдал отказа, в результате которого перестал бы работать контур управления температурой. Группа АСЗ принимает решение, что средняя вероятность отказа при наличии запроса составляет 0,1, и вносит значение 0,1 в колонку «ОСУП» графы 5 на рисунке F.1 (0,1 — это минимально допустимое значение для ОСУП).

F.14.6 Аварийная сигнализация

Система имеет в своем составе датчик расхода охлаждающей воды в конденсатор. Этот датчик подключен к разным входам ОСУП и контроллера регулирования температуры. При малом потоке охлаждающей воды в конденсатор срабатывает аварийная сигнализация, требующая от оператора вмешаться в ход процесса и перекрыть подачу пара. Аварийная сигнализация может считаться слоем защиты, так как она размещается в другом по отношению к контуру регулирования температуры контроллере ОСУП. Группа АСЗ принимает решение, что и в этом случае среднюю вероятность отказа при запросе можно принять равной 0,1, так как оператор всегда находится в операторском помещении. В колонку «Сигнализация» графы 5 на рисунке F.1 заносят значение 0,1.

F.14.7 Дополнительное ослабление

Во время работы установки доступ в рабочую зону ограничен. Обслуживание производят только в те периоды, когда оборудование остановлено и отключено. План безопасного ведения процесса требует, чтобы все лица, не относящиеся к оперативному персоналу, отмечались при входе в рабочее помещение и предупреждали о своем приходе оператора. Группа АСЗ полагает, что наличие таких усиленных ограничений доступа приводит к снижению риска для оперативного персонала на порядок. Поэтому в графу 6 «Дополнительное ослабление, ограничение доступа» на рисунке F.1 вводят значение 0,1.

F.14.8 Независимый слой защиты (НСЗ)

Реактор оборудован предохранительным клапаном, рассчитанным таким образом, чтобы пропустить весь объем газа, образовавшегося за период повышения температуры и давления, вызванного отсутствием охлаждающей воды. Далее с учетом запасов и состава материала был оценен вклад предохранительного клапана в снижение риска. Поскольку предохранительный клапан настроен на давление ниже расчетного давления фиберглассовой колонны и ошибка оператора, в результате которой колонна во время работы была бы изолирована от предохранительного клапана, невозможна, предохранительный клапан рассматривается как слой защиты. Сам предохранительный клапан демонтируют и испытывают каждый год, и ни разу за 15 лет работы не наблюдалось забивания клапана или смежных труб. Так как предохранительный клапан соответствует критерию НСЗ, то оценка средней вероятности отказа при запросе принята равной 0,01 и соответствующее значение занесено в графу 7 на рисунке F.1.

F.14.9 Возможность промежуточного события

Числа, занесенные в первую строку всех граф, перемножают и результат заносят в графу 8 «Вероятность промежуточного события» на рисунке F.1. Произведение этих величин в настоящем примере составляет 10^{-7}.

F.14.10 ПСБ

Ослабление и снижение риска, полученные благодаря слоям защиты, оказываются достаточными, чтобы удовлетворить корпоративному критерию. Можно, однако, получить дальнейшее ослабление, причем при минимальных затратах, поскольку в системе предусмотрены датчик давления в сосуде, а также соответствующая сигнализация в ОСУП. Группа АСЗ принимает решение ввести дополнительную функцию безопасности ПСБ, которая состоит из выключателя и реле, прекращающих подачу питания на соленоидный клапан, связанный с клапаном на линии подачи пара в рубашку реактора. Эта функция безопасности ПСБ имеет низший уровень полноты безопасности (УПБ 1), и ее средняя вероятность отказа при запросе равна 0,01. Значение 0,01 вносят в графу 9 «УПБ функции безопасности ПСБ» на рисунке F.1.

Затем рассчитывают вероятность ослабления влияющего события. Этого достигают путем перемножения чисел в графах 8 и 9. Результат, равный 1×10^{-9}, заносят в графу 10 на рисунке F.1.

F.14.11 Следующая функция безопасности ПСБ

Затем группа АСЗ рассматривает вторую исходную причину (отказ контура управления расходом пара в реакторе). Вероятность отказа управляющего клапана определяют по таблице F.3 и в графу 4 «Вероятность появления исходной причины» на рисунке F.1 вносят число 0,1.

Слои защиты, предусмотренные при проектировании процесса, аварийная сигнализация, дополнительное ослабление и ПСБ — все это также служит защитой при отказе контура управления паром. Единственный отсутствующий слой защиты — это ОСУП. Группа АСЗ рассчитывает промежуточную вероятность (1×10^{-6}) и вероятность ослабления влияющего события (1×10^{-8}). Эти величины вносят соответственно в графы 8 и 10 на рисунке F.1.

Группа АСЗ будет продолжать анализ до тех пор, пока не будут рассмотрены все отклонения, обнаруженные методом HAZOP.

Заключительный шаг — сложение вероятностей ослабления влияющих событий для событий с серьезными и высокими уровнями тяжести, которые вызваны той же опасностью.

В настоящем примере, если бы для всего процесса было выявлено только одно влияющее событие, эта величина была бы равной $1{,}1 \times 10^{-8}$. Так как вероятность воспламенения была рассчитана по данным проекта (0,1), а вероятность пребывания людей в опасной зоне с учетом дополнительного ослабления составляет (0,1), то уравнение для риска фатального исхода, вызванного пожаром, сводится к следующему:

риск фатального исхода от пожара = (общая вероятность ослабления влияющих событий, связанных с выбросом воспламеняющегося материала) $\times$ (вероятность получения фатальной травмы при пожаре)

или риск фатального исхода от пожара = $(1{,}1 \times 10^{-8}) \times (0{,}5) = 5{,}5 \times 10^{-9}$.

Это число ниже корпоративного критерия для данной опасности, и дальнейшее снижение риска не является экономически оправданным. Таким образом, работу группы АСЗ можно считать завершенной.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61508	IDT	ГОСТ Р МЭК 61508—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
МЭК 61511-1	IDT	ГОСТ Р МЭК 61511-1—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»
МЭК 61511-2	IDT	ГОСТ Р МЭК 61511-2—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1»
МЭК 61508-5	IDT	ГОСТ Р МЭК 61508-5—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»

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

- IDT — идентичные стандарты.

Библиография

[1] Reducing Risks, Protecting People, HSE London, 2001 (ISBN 0 7176 2151 0).

[2] Assessment principles for offshore safety cases, HSE London, 1998 (ref. HSG 181) (ISBN 0 7176 1238 4)

[3] Safety assessment principles for nuclear plants, HSE London, 1992 (ISBN 0 11 882043 5)

[4] Tolerability of risks from nuclear power stations, HMSO London, 1992 (ISBN 0 11 886368 1)

[5] The use of computers in safety-critical applications. Health and Safety Commission, London, 1998 (ISBN 0 7176 1620 7)

[6] CONTINI, S. Benchmark Exercise on Major Hazard Analysis, Commission of European Communities, 1992

[7] A process industry view of IEC 61508, Dr. A.G. King, IEE Computing and Control Engineering Journal, February 2000, Institution of Electrical Engineers, London, 2000

[8] Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1

[9] ISA-S91.01-1995, Identification of Emergency Shutdown Systems and Controls That are Critical to Maintaining Safety in Process Industries, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA

[10] Safety Shutdown Systems: Design, Analysis and Justification, Gruhn and Cheddie, 1998, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA, ISBN 1-55617-665-1

[11] FM Global Properly Loss Prevention Data Sheet 7-45, «Instrumentation and Control in Safety Applications», 1998, FM Global, Johnston, RI, USA

[12] DIN V 19250, 1994: Control technology: Fundamental safety aspects to be considered for measurement and control equipment

[13] VDI/VDE 2180 Safeguarding of industrial process plants by means of process control engineering

УДК 62-783:614.8:331.454:006.354 ОКС 25.040.01 Т51

Ключевые слова: безопасность функциональная, жизненный цикл систем, приборные системы безопасности, риск, полнота безопасности, слои защиты, принцип ALARP, граф риска

Редактор *А.Д. Чайка*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 02.11.2012. Подписано в печать 22.11.2012. Формат 60x84 1/8. Гарнитура Ариал. Усл. печ. л. 5,12. Уч.-изд. л. 4,70. Тираж 93 экз. Зак. 1052.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.