МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34332.1— 2017

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 1

Основные положения

(IEC 61508-4:2010, NEQ)
(IEC 61508-5:2010, NEQ)
(ISO/IEC Guide 51:2014, NEQ)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Всемирная Академия наук комплексной безопасности» (АНО «ВАН КБ»)

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 ноября 2017 г. № 52)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 829-ст межгосударственный стандарт ГОСТ 34332.1—2017 введен в действие в качестве национального стандарта Российской Федерации с 1 марта 2019 г.

5 В настоящем стандарте учтены основные нормативные положения следующих международных стандартов и документов:

IEC 61508-4:2010 «Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 4. Термины и сокращения» («Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations», NEQ);

IEC 61508-5:2010 «Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности» («Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels», NEQ);

ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты» («Safety aspects: Guidelines for their inclusion in standards», NEQ)

6 Настоящий стандарт подготовлен на основе применения ГОСТ Р 53195.1—2008*

7 ВВЕДЕН ВПЕРВЫЕ

* Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 829-ст ГОСТ Р 53195.1—2008 отменен с 1 марта 2019 г.

*Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном 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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 7
5 Общие положения 7
6 Проектные опасности 10
7 Риск 10
8 Принципы установления приемлемого риска 14
9 Определение уровней полноты безопасности 14
Приложение А (справочное) Системы 15
Приложение Б (справочное) Источники, виды и характер опасностей 17
Приложение В (справочное) Факторы риска 18
Приложение Г (справочное) Критерии и категории тяжести последствий 20
Приложение Д (справочное) Основные понятия риска и полноты безопасности 21
Приложение Е (справочное) Выбор методов для определения требований к уровню полноты безопасности 29
Приложение Ж (справочное) Принцип разумной достаточности и концепция приемлемого риска . . 31
Приложение И (справочное) Определение уровня полноты безопасности. Количественный метод 33
Приложение К (справочное) Определение уровня полноты безопасности. Методы, основанные на графе рисков 35
Приложение Л (справочное) Определение уровня полноты безопасности. Полуколичественный метод с использованием анализа слоя защиты 41
Приложение М (справочное) Определение уровня полноты безопасности. Качественный метод — матрица тяжести последствий опасных событий 45
Библиография 47

Введение

Современные здания и сооружения — объекты капитального строительства — представляют собой сложные системы, в состав которых входит система строительных конструкций и ряд инженерных систем в разных сочетаниях, в том числе для жизнеобеспечения, реализации технологических процессов, энерго- и ресурсосбережения, обеспечения безопасности и другие системы. Эти системы взаимодействуют друг с другом, с внешней и внутренней средами и вместе действуют как единое целое, выполняя свои функции назначения.

Объекты капитального строительства жестко привязаны к местности. Рабочие характеристики зданий, сооружений и входящих в них систем могут быть реализованы, проверены и использованы только в том месте, в котором объекты построены и системы установлены.

Безопасность зданий и сооружений обеспечивается применением совокупности мер, мероприятий и средств снижения риска причинения вреда до уровня приемлемого риска и поддержания этого уровня в течение периода эксплуатации или использования этих объектов. К средствам снижения риска относятся системы, связанные с безопасностью зданий и сооружений (СБЗС системы). Среди СБЗС систем наиболее распространенными являются системы, содержащие электрические и/или электронные, и/или программируемые электронные (Э/Э/ПЭ) компоненты. Такие системы, именуемые Э/Э/ПЭ СБЗС системами, в течение многих лет используются для выполнения функций безопасности. Кроме них и вместе с ними используются системы, основанные на неэлектрических (гидравлических, пневматических) технологиях, а также прочие средства уменьшения риска. Для решения задач безопасности зданий и сооружений во всех больших объемах используются программируемые электронные СБЗС системы.

Следующими по важности характеристиками систем, после характеристик назначения, являются характеристики безопасности. Важнейшей характеристикой безопасности систем признана их функциональная безопасность.

В настоящем стандарте установлены термины с их определениями, общие положения, относящиеся к функциональной безопасности Э/Э/ПЭ СБЗС систем, принципы установления приемлемого риска и определения полноты безопасности систем с учетом источников, видов, характера опасностей, факторов риска и тяжести последствий.

Стандарт ориентирован на обеспечение соблюдения требований безопасности зданий и сооружений, в том числе объектов транспортных инфраструктур, установленных техническими регламентами Таможенного союза [1] — [3], а также Техническим регламентом Евразийского экономического союза [4] (после его вступления в силу) и в развитие базовых требований этих технических регламентов.

Настоящий стандарт распространяется на любые Э/Э/ПЭ СБЗС системы и на составляющие этих систем, включая сенсоры, исполнительные устройства и интерфейс «человек — машина». Он рассчитан на любой диапазон сложности Э/Э/ПЭ СБЗС систем и ориентирован на комплексное обеспечение безопасности зданий и сооружений гражданского и промышленного строительства, включая объекты инфраструктур промышленности и энергетики, транспорта и связи, гидротехнических и мелиоративных сооружений.

Настоящий стандарт входит в комплекс стандартов с наименованием «Безопасность функциональная систем, связанных с безопасностью зданий и сооружений» и является первым стандартом этого комплекса — Часть 1. Основные положения. Другие стандарты, входящие в этот комплекс:

Часть 2. Общие требования;

Часть 3. Требования к системам;

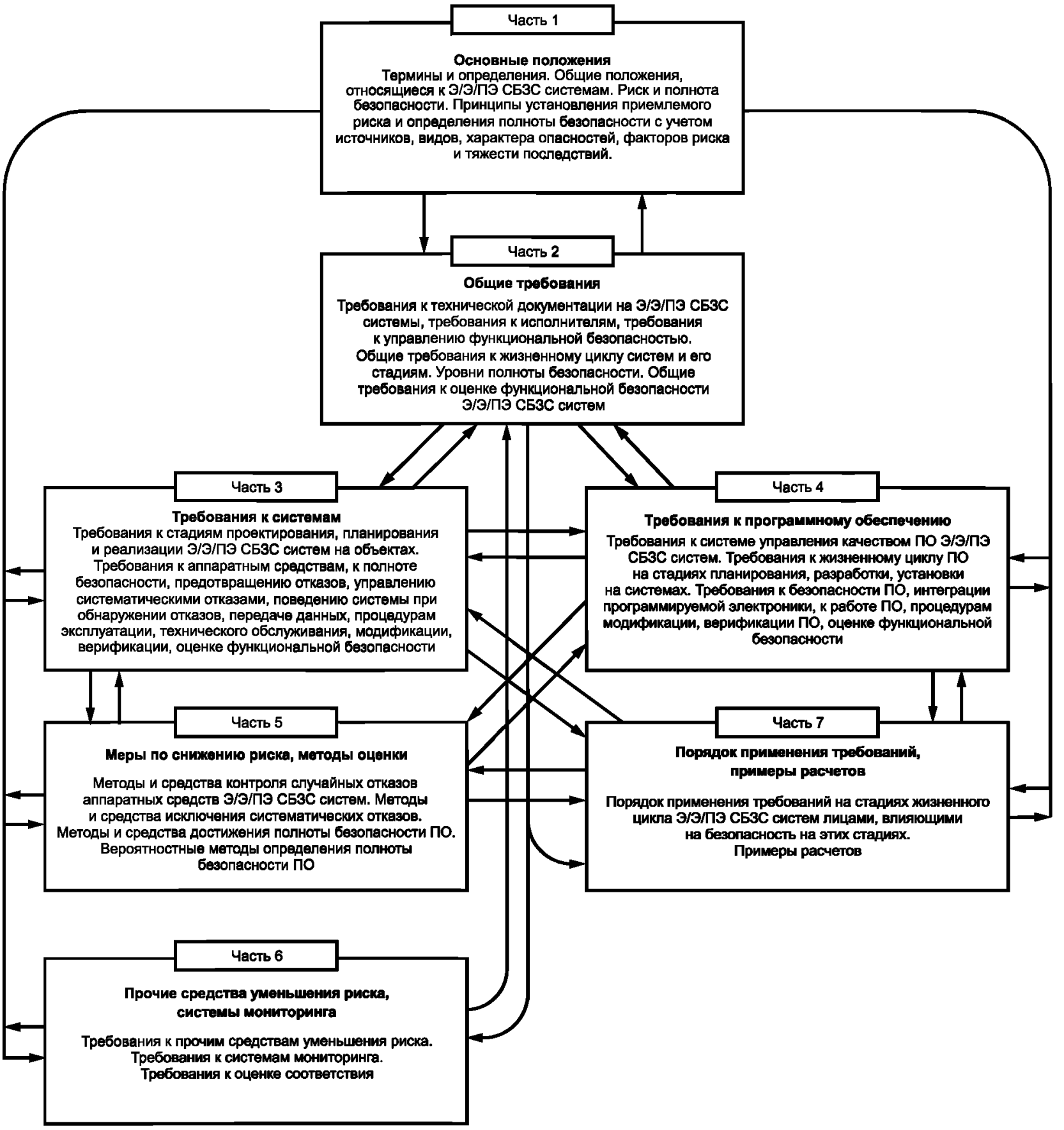
Часть 4. Требования к программному обеспечению;

Часть 5. Меры по снижению риска, методы оценки;

Часть 6. Внешние средства уменьшения риска, системы мониторинга;

Часть 7. Порядок применения требований, примеры расчетов.

Структура комплекса стандартов приведена ниже.


Часть 1
Основные положения
Термины и определения. Общие положения, относящиеся к Э/Э/ПЭ СБЗС системам. Риск и полнота безопасности. Принципы установления приемлемого риска и определения полноты безопасности с учетом источников, видов, характера опасностей, факторов риска и тяжести последствий.
Часть 2
Общие требования
Требования к технической документации на Э/Э/ПЭ СБЗС системы, требования к исполнителям, требования к управлению функциональной безопасностью. Общие требования к жизненному циклу систем и его стадиям. Уровни полноты безопасности. Общие требования к оценке функциональной безопасности Э/Э/ПЭ СБЗС систем
Часть 3
Требования к системам
Требования к стадиям проектирования, планирования и реализации Э/Э/ПЭ СБЗС систем на объектах. Требования к аппаратным средствам, к полноте безопасности, предотвращению отказов, управлению систематическими отказами, поведению системы при обнаружении отказов, передаче данных, процедурам эксплуатации, технического обслуживания, модификации, верификации, оценке функциональной безопасности
Часть 4
Требования к программному обеспечению
Требования к системе управления качеством ПО Э/Э/ПЭ СБЗС систем. Требования к жизненному циклу ПО на стадиях планирования, разработки, установки на системах. Требования к безопасности ПО, интеграции программируемой электроники, к работе ПО, процедурам модификации, верификации ПО, оценке функциональной безопасности
Часть 5
Меры по снижению риска, методы оценки
Методы и средства контроля случайных отказов аппаратных средств Э/Э/ПЭ СБЗС систем. Методы и средства исключения систематических отказов. Методы и средства достижения полноты безопасности ПО. Вероятностные методы определения полноты безопасности ПО
Часть 7
Порядок применения требований, примеры расчетов
Порядок применения требований на стадиях жизненного цикла Э/Э/ПЭ СБЗС систем лицами, влияющими на безопасность на этих стадиях. Примеры расчетов
Часть 6
Прочие средства уменьшения риска, системы мониторинга
Требования к прочим средствам уменьшения риска. Требования к системам мониторинга. Требования к оценке соответствия

13 ОХРАНА ОКРУЖАЮЩЕЙ СРЕДЫ, ЗАЩИТА ЧЕЛОВЕКА ОТ ВОЗДЕЙСТВИЯ ОКРУЖАЮЩЕЙ СРЕДЫ. БЕЗОПАСНОСТЬ

МКС 13.100,
13.110,
13.200,
13.220,
13.310,
13.320,
91.120.99

Поправка к ГОСТ 34332.1—2017 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 1. Основные положения

В каком месте	Напечатано	Должно быть
Предисловие. Пункт 6.	ГОСТ Р 53195.1—2008*	ГОСТ Р 53195.1—2008
Сноска — *	———— * Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 829-ст ГОСТ Р 53195.1—2008 отменен с 1 марта 2019 г.	—

(ИУС № 1 2020 г.)

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 1

Основные положения

Functional safety of building/construction safety-related systems. Part 1. General

Дата введения — 2019—03—01

1 Область применения

1.1 Настоящий стандарт устанавливает:

- термины и определения в области функциональной безопасности систем, связанных с безопасностью зданий и сооружений (далее — СБЗС систем), адаптированные к строительной отрасли;
- основные положения по определению требований к функциональной безопасности электрических, электронных, программируемых электронных систем, связанных с безопасностью зданий и сооружений (далее — Э/Э/ПЭ СБЗС систем);
- принципы и процедуры определения, установления и достижения приемлемого уровня полноты безопасности Э/Э/ПЭ СБЗС систем в условиях опасных воздействий природного, техногенного и антропогенного характера на здание или сооружение и его составляющие с применением Э/Э/ПЭ СБЗС систем;
- виды применяемых Э/Э/ПЭ СБЗС систем;
- источники, виды и характер опасностей;
- факторы риска, критерии и категории тяжести последствий;
- методы, рекомендуемые для определения требований к уровню полноты безопасности в различных условиях применения.

1.2 Настоящий стандарт распространяется на Э/Э/ПЭ СБЗС системы, включая комплексные системы безопасности (далее — КСБ), устанавливаемые или установленные во вновь возводимых или реконструируемых зданиях и сооружениях (именуемых также в настоящем стандарте объектами) всех отраслей экономики независимо от форм собственности и ведомственной принадлежности, включая жилые, общественные и производственные здания и сооружения, в том числе на Э/Э/ПЭ СБЗС системы объектов инфраструктуры перерабатывающей промышленности, энергетики, транспорта, гидротехнических и мелиоративных сооружений.

Настоящий стандарт не распространяется на Э/Э/ПЭ СБЗС систему, которая является единственной одиночной системой, способной осуществить необходимое снижение риска на объекте, и требуемая полнота безопасности этой системы ниже, чем определено уровнем полноты безопасности УПБ 1 — самым низким уровнем полноты безопасности по ГОСТ 34332.2 (таблицы 1 и 2).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие межгосударственные стандарты:

ГОСТ ISO 9000—2011 Системы менеджмента качества. Основные положения и словарь

ГОСТ ISO 9001—2011 Системы менеджмента качества. Требования

Издание официальное

ГОСТ 34332.2—2017 Безопасность функциональная систем, связанных с безопасностью зданий и сооружений. Часть 2. Общие требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежегодного информационного указателя «Национальные стандарты» за текущий год. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **акт незаконного вмешательства:** Противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности объекта, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий.

3.2 **анализ риска** (risk analysis): Систематическое использование имеющейся информации для выявления опасностей и для оценки риска.

3.3 **антропогенная опасность:** Опасность, исходящая от людей, вызванная их непреднамеренными действиями (такими, как ошибки, неправильное использование оборудования и др.), бездействием или злонамеренными действиями (такими, как хищение, саботаж, диверсия, нападение, терроризм).

3.4 **аудит функциональной безопасности** (functional safety audit): Систематическое и независимое исследование, осуществляемое для определения правильности реализации запланированных мероприятий, предназначенных для достижения и поддержания предусмотренного уровня полноты безопасности связанных с безопасностью систем или системы.

3.5 **вред** (harm): Физическое повреждение или урон, причиненные здоровью или жизни человека, имуществу, окружающей среде.

3.6 **вторжение** (intrusion): Несанкционированное проникновение на охраняемую или контролируемую территорию, зону или объект.

3.7 **жизненный цикл системы, связанной с безопасностью зданий и сооружений**; жизненный цикл СБЗС системы (safety life cycle): Последовательность следующих друг за другом необходимых процессов создания и использования системы, связанной с безопасностью здания или сооружения, проходящих в течение интервала времени, который начинается со стадии разработки концепции проекта системы и заканчивается, когда эта система выведена из эксплуатации и утилизирована.

3.8 **жизненный цикл программного обеспечения**; жизненный цикл ПО (software lifecycle): Последовательность следующих друг за другом процессов создания и использования программного обеспечения программируемой системы, связанной с безопасностью здания или сооружения, происходящих в течение интервала времени, который начинается с разработки общей концепции программного обеспечения и заканчивается, когда программное обеспечение окончательно выведено из эксплуатации.

3.9 **инженерная система [подсистема] здания [сооружения]:** Система [подсистема] здания [сооружения], предназначенная для жизнеобеспечения, выполнения процессов, поддержания комфорта, энерго- и ресурсосбережения или обеспечения безопасности.

Примечание — В состав инженерной системы [подсистемы] здания [сооружения] может входить человек (оператор, пользователь).

3.10 **использование по назначению** (intended use): Использование здания или сооружения, системы или средства в соответствии с информацией, предоставленной застройщиком, поставщиком системы или средства, либо поставщиком услуг по их использованию, содержащейся в утвержденной в установленном порядке эксплуатационной документации.

3.11 **комплексная система безопасности**; КСБ: Система безопасности, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей.

3.12 **комплексное обеспечение безопасности:** Обеспечение безопасности при наличии нескольких видов и/или источников опасности.

3.13 **максимально допустимый риск:** Максимальное установленное значение приемлемого риска.

3.14 **мера безопасности** (safety measure): Мера, применяемая для снижения риска.

Примечание — Снижение риска может быть достигнуто за счет выполнения норм и правил и/или выбора эффективных проектных решений, и/или применения связанных с безопасностью систем, прочих средств уменьшения риска, персональных защитных средств, и/или за счет предоставления необходимой информации по установке и применению связанных с безопасностью систем и средств производителям работ, эксплуатирующему персоналу и пользователям, а также за счет их обучения и тренировок.

3.15 **модель нарушителя:** Совокупность параметров и характеристик, свойственных потенциальному нарушителю, определяющих его вероятные действия.

3.16 **нарушитель** (intruder): Лицо, осуществляющее попытку акта незаконного вмешательства или несанкционированного действия либо осуществившее такие действия.

3.17 **недопустимый риск** (unacceptable risk): Риск, который не может быть оправдан ни при каких обычных обстоятельствах.

3.18 **необходимое снижение риска** (necessary risk reduction): Снижение риска, которое должно быть достигнуто связанными с безопасностью системами и прочими средствами уменьшения риска для гарантии того, что уровень допустимого риска не будет превышен.

3.19 **несанкционированное действие:** Действие лица, осуществляемое без предусмотренного специального разрешения или вопреки запрету.

3.20 **общепризнанная методика:** Методика испытаний, измерений, оценки или расчетов, признанная международным (региональным) профессиональным сообществом пригодной для практического использования в конкретной области применения.

3.21 **окружение** (environment): Все системы, средства и окружающая среда, вокруг связанной с безопасностью системы (ее составляющих), которые могут повлиять на достижение ее функциональной безопасности в конкретном рассматриваемом применении и на любой стадии жизненного цикла этой системы.

3.22 **опасная ситуация** (hazardous situation): Обстоятельство, при котором люди, имущество или окружающая среда подвергаются(ется) одной или более опасностей.

3.23 **опасное событие** (hazardous event): Опасная ситуация, которая может привести к причинению вреда.

3.24 **опасность** (hazard): Потенциальный источник причинения вреда.

3.25 **опасный отказ** (dangerous failure): Отказ, приводящий связанную с безопасностью систему в опасное состояние или к ошибке при выполнении функции безопасности.

3.26 **особо опасный объект:** Объект, на котором используют, производят, перерабатывают, хранят, транспортируют или уничтожают радиоактивные пожаровзрывоопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации.

3.27 **остаточный риск** (residual risk): Риск, оставшийся после принятия мер безопасности.

3.28 **оценка риска** (risk assessment): Общий процесс, включающий в себя анализ риска и оценку риска.

3.29 **оценивание риска** (risk evaluation): Процедура, основанная на анализе риска для определения, был ли превышен допустимый риск.

3.30 **оценка функциональной безопасности** (functional safety assessment): Исследование, основанное на фактах, выполняемое по утвержденной в установленном порядке методике, предназначенное для определения значения полноты безопасности СБ систем и средств, обеспечивающих выполнение заданной функции или функций безопасности.

3.31 **ошибка человека [оператора], [пользователя]** (human error): Действие человека [оператора], [пользователя], приведшее к непредусмотренному результату.

3.32 **полнота безопасности (системы)** (safety integrity): Вероятность успешного выполнения СБ системой функции или функций безопасности в конкретных условиях и в пределах конкретного интервала времени.

Примечания

1 Чем выше УПБ, тем ниже вероятность того, что СБ система не сможет выполнить заданную(ые) функцию(ии) безопасности или не будет в состоянии, когда потребуется, принять определенное состояние.

2 Существует четыре УПБ для систем (см. 3.52).

3 Полнота безопасности СБ системы включает в себя полноту безопасности аппаратных средств (АС) и полноту безопасности по отношению к систематическим отказам.

3.33 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности связанной с безопасностью системы по отношению к отказам аппаратных средств, проявляющимся в опасном режиме при заданных условиях и в пределах заданного интервала времени.

3.34 **полнота безопасности программного обеспечения**; полнота безопасности ПО (software safety integrity): Составляющая полноты безопасности связанной с безопасностью системы, относящаяся к систематическим отказам програмного обеспечения, проявляющимся в опасном режиме.

3.35 **полнота безопасности при систематических отказах** (systematic safety integrity): Составляющая полноты безопасности связанной с безопасностью системы, относящаяся к систематическим отказам, проявляющимся в опасном режиме.

Примечание — Обычно полнота безопасности, касающаяся систематических отказов, не может быть охарактеризована количественно (в отличие от полноты безопасности аппаратных средств, которая, как правило, может быть оценена количественно).

3.36 **предсказуемое неправильное использование** (reasonably foreseeable misuse): Использование здания, сооружения, системы, средства для целей, не предусмотренных застройщиком или поставщиком средства, либо поставщиком услуг по их использованию, но которое может быть следствием легко предсказуемого поведения человека.

3.37 **приемлемый риск** (tolerable risk): Риск, который считается обычным при данных обстоятельствах, на основе существующих в текущий период времени ценностей и возможностей общества и государства.

Примечание — В технических нормах часто применяют термин «допустимый риск», который является синонимом «приемлемого риска», примененного в настоящем стандарте.

3.38 **природная опасность:** Опасность, источником которой является природное явление (например, землетрясение, лавина, сель, оползень, вулканическая деятельность, наводнение, подтопление, гроза, ураган, обледенение).

3.39 **программируемая электронная система** (programmable electronic system; PES): Система, предназначенная для управления, защиты или мониторинга, содержащая одно или несколько программируемых электронных устройств, включая все элементы системы, такие как источники питания, сенсоры и устройства ввода, каналы передачи данных и коммуникационные магистрали, приводы и оконечные устройства.

3.40 **проектная опасность:** Опасность, предусмотренная при проектировании и учитываемая на стадиях жизненных циклов объекта и систем при оценке и подтверждении соответствия требованиям безопасности.

3.41 **прочее средство уменьшения риска** (other risk reduction measure): Средство уменьшения или смягчения риска, отдельное и отличное от системы, связанной с безопасностью здания или сооружения, и не содержащее такой системы.

Пример — Огнезащитная преграда, ограждение являются прочими средствами уменьшения риска.

3.42 **разнообразие** (diversity): Признак, относящийся к средствам и характеризующий различие методов, применяемых для получения требуемой функции.

Пример — Разнообразие может достигаться использованием различных физических методов и различных проектных подходов.

3.43 **риск** (risk): Сочетание вероятности возникновения вреда и тяжести этого вреда.

Примечание — Вероятность возникновения включает в себя продолжительность воздействия опасной ситуации, возникновение опасного события, а также возможность избежать или ограничить вред.

3.44 **связанная с безопасностью система [подсистема]**; СБ система (safety-related system): Система [подсистема], реализующая функцию или функции безопасности, необходимые для достижения и поддержания безопасного состояния управляемого оборудования самостоятельно или совместно с другими связанными с безопасностью системами или прочими средствами уменьшения риска.

Примечания

1 Настоящий термин относится к системам, обозначенным как связанные с безопасностью системы (СБ системы), предназначенным для снижения риска до уровня приемлемого риска самостоятельно или совместно с прочими средствами уменьшения риска.

2 СБ системы предназначены для предотвращения перехода управляемого оборудования в опасное состояние путем выполнения необходимых действий при обнаружении условий, которые могут привести к опасному событию. СБ системы могут быть разделены на две категории: СБ системы управления и СБ системы защиты.

3 СБ системы могут быть составной частью системы управления управляемого оборудования либо могут быть связаны с управляемым оборудованием с помощью датчиков и/или исполнительных устройств. Т. е., необходимый уровень полноты безопасности может быть достигнут реализацией функций безопасности в системе управления управляемым оборудованием, либо они могут быть реализованы отдельными, независимыми СБ системами.

4 СБ система может быть предназначена:

- для предотвращения опасного события (т. е., если связанная с безопасностью система выполняет свои функции безопасности, то опасного события не происходит);
- для смягчения последствий опасного события (снижая риски путем уменьшения тяжести последствий);
- для достижения целей, указанных в первом и втором перечислениях).

5 Человек (оператор) может быть частью СБ системы.

6 СБ система включает в себя аппаратные средства, программное обеспечение и дополнительные средства (например, источники питания, датчики, устройства ввода/ввода, исполнительные элементы и др.).

7 Связанная с безопасностью система может быть основана на широком диапазоне технологий, включая электрическую, электронную, программируемую электронную, гидравлическую, пневматическую технологии.

8 СБ подсистема в настоящем термине также является системой, которая входит составной частью в более крупную систему; подсистема, в свою очередь, может состоять из менее крупных подсистем, которые также являются системами. При этом каждая из рассмотренных подсистем является СБ системой, реализующей определенную функцию или функции безопасности.

3.45 **связанный с управляемым оборудованием риск**; связанный с УО риск (EUC risk): Риск, обусловленный применением управляемого оборудования и его взаимодействием с системой управления управляемым оборудованием.

Примечания

1 В данном контексте риск связан с конкретным опасным событием, в котором для необходимого снижения риска используют системы, связанные с безопасностью здания или сооружения, и применяют прочие средства уменьшения риска (т. е. риск связан с функциональной безопасностью).

2 Основной целью определения риска, связанного с управляемым оборудованием, является установление понятия риска без учета СБЗС систем и прочих средств уменьшения риска.

3 Оценка этого риска включает в себя вопросы учета человеческого фактора.

3.46 **система мониторинга инженерных систем (здания или сооружения):** Совокупность аппаратно-программных средств для регулярного наблюдения и регистрации состояния и функционирования инженерных систем здания или сооружения.

3.47 **система мониторинга строительных конструкций:** Совокупность аппаратно-программных средств для регулярного наблюдения и регистрации состояния строительных конструкций здания или сооружения.

3.48 **система [подсистема], связанная с безопасностью зданий и сооружений**; СБЗС система [подсистема]: Связанная с безопасностью система [подсистема], установленная в здании или сооружении, взаимодействующая с системами или подсистемами этих объектов, с их составляющими и окружением.

Примечание — Под окружением в данном контексте понимается все, что может повлиять на достижение функциональной безопасности СБЗС системы в конкретном рассматриваемом применении (например, физическая, эксплуатационная, правовая среды и среда обслуживания) и для любой стадии ее жизненного цикла.

3.49 **система телевизионного наблюдения**; система ТВ наблюдения (CCTV-system): Система замкнутого телевидения, предназначенная для телевизионной съемки контролируемой зоны или зон, передачи, приема, отображения, обработки, записи (документирования) и воспроизведения телевизионного сигнала с целью наблюдения и изучения объектов, субъектов и событий съемки.

Примечания

1 В состав телевизионного сигнала системы ТВ наблюдения обычно входят: сигнал изображения, идентификатор телевизионной камеры, дата и время съемки.

2 В состав телевизионного сигнала цифровой системы ТВ наблюдения могут входить видеоданные (сигнал изображения), звукоданные (сигнал звука), метаданные (служебная информация: дата, время, идентификатор ТВ камеры и другая информация с широким спектром применения, в том числе содержащая запрет на внесение необнаруживаемых изменений).

3.50 **система управления управляемым оборудованием**; система управления УО (equipment under control of control system; EUC control system): Система, реагирующая на входные сигналы, поступающие от процесса и/или от оператора, и генерирующая выходные сигналы, которые обеспечивают выполнение управляемым оборудованием необходимого действия.

3.51 **техногенная опасность:** Опасность, обусловленная объектами, созданными людьми, и/или процессами их деятельности.

3.52 **уровень полноты безопасности**; УПБ (safety integrity level; SIL): Дискретный уровень, принимающий одно из четырех возможных значений, определяющий требования к полноте безопасности связанной с безопасностью системы.

Примечания

1 Уровни полноты безопасности СБ систем определяются вероятностью или частотой отказов по запросу и установлены в ГОСТ 34332.2 (таблицы 1 и 2).

2 Уровень полноты безопасности 4 характеризует наибольшую полноту безопасности, УПБ 1 — наименьшую полноту безопасности.

3.53 **уязвимая группа пользователей** (vulnerable users): Группа пользователей, подвергаемых большему риску причинения вреда со стороны здания, сооружения, системы или средства из-за возраста, уровня грамотности, физического или психического состояния, либо ограничений или невозможности доступа к информации о безопасности.

3.54 **функциональная безопасность** (functional safety): Часть безопасности, относящаяся к управляемому оборудованию и системе управления управляемым им, которая зависит от правильного функционирования связанной с безопасностью системы и прочих средств уменьшения риска при выполнении функции безопасности.

3.55 **функция безопасности:** Функция, реализуемая электрической/электронной/программируемой электронной системой или системой снижения риска на основе неэлектрических технологий, которая предназначена для достижения или поддержания безопасного состояния управляемого оборудования по отношению к конкретному опасному событию.

Примечание — Функция безопасности характеризуется назначением (функционалом выполнения функции) и полнотой безопасности.

3.56 **целевой риск** (target risk): Значение риска, которое намереваются достигнуть (получить) для конкретной опасности с учетом риска, обусловленного применением управляемого оборудования совместно с Э/Э/ПЭ СБЗС системами и применением прочих средств уменьшения риска.

3.57 **электрическая/электронная/программируемая электронная система**; Э/Э/ПЭ система (electrical/electronic/programmable electronic system; E/E/PES): Электрическая и/или электронная, и/или программируемая электронная система, предназначенная для управления, защиты или мониторинга, содержащая одно или несколько электрических и/или электронных, и/или программируемых электронных устройств.

Примечание — Обычно в состав Э/Э/ПЭ системы включены все ее элементы, такие как источники питания, сенсоры, входные устройства, устройства ввода, устройства обработки данных, коммуникационные магистрали, устройства вывода, устройства привода, выходные или оконечные устройства.

3.58 **электрическая/электронная/программируемая электронная система, связанная с безопасностью здания [сооружения]**; Э/Э/ПЭ СБЗС система: Электрическая и/или электронная, и/или программируемая электронная система, спроектированная и установленная в здании [сооружении] как его неотъемлемая часть, предназначенная для снижения риска причинения вреда и/или тяжести последствий.

Примечание — В данном контексте словосочетание «причинение вреда» относится к жизни и здоровью людей, пребывающих в здании [сооружении] и окружающей территории, имуществу, жизни и здоровью животных и растений, окружающей среде.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и обозначения:

АС — аппаратное средство;

АСЗ — анализ слоя защиты;

ЕАЭС — Евразийский экономический союз;

КСБ — комплексная система безопасности;

ПО — программное обеспечение;

СБ система — связанная с безопасностью система;

СБЗС система — связанная с безопасностью здания или сооружения система;

СЗ — слой защиты;

ТР — технический регламент;

ТР ТС — технический регламент Таможенного союза;

ТС — Таможенный союз;

УО — управляемое оборудование;

УПАТС — управленческая автоматическая телефонная станция;

УПБ — уровень полноты безопасности;

Э/Э/ПЭ — и/или электронная, и/или программируемая электронная (в отношении системы или ее составляющей);

Э/Э/ПЭ СБЗС система — электрическая и/или электронная, и/или программируемая система, связанная с безопасностью здания или сооружения;

УКВ ЧМ/FM — обозначение стандарта ультракоротковолнового радиовещания с частотной модуляцией (полярной модуляцией — ЧМ, с пилот-тоном — FM).

5 Общие положения

5.1 Здание, сооружение как система

В рамках настоящего стандарта здание или сооружение (объект строительного производства) рассматривают как сложную систему, включающую в себя систему строительных конструкций, инженерные системы в различных сочетаниях для жизнеобеспечения, реализации процессов, энерго- и ресурсосбережения, обеспечения безопасности (модель здания или сооружения как сложной системы представлена на рисунке 1). Системы, входящие в состав здания или сооружения, взаимодействуют между собой, с внешним и внутренним окружением. Здание или сооружение взаимодействует с внешним окружением на градостроительном, ресурсном, структурном, функциональном, информационном уровнях с учетом географических, геологических, климатических и иных местных условий.

Э/Э/ПЭ СБЗС системы, входящие в состав здания или сооружения, выполняют функции безопасности и снижают риск причинения вреда жизни и здоровью людей (животных, растений), имуществу, окружающей среде.

Для обеспечения безопасности здания или сооружения наряду с Э/Э/ПЭ СБЗС системами и вместе с ними могут быть применены СБЗС системы, основанные на неэлектрических технологиях, и прочие средства уменьшения риска.

5.2 Составляющие зданий и сооружений

5.2.1 Система строительных конструкций

В систему строительных конструкций здания или сооружения входят в различных сочетаниях элементы, влияющие на безопасность объекта, приведенные в А.1 (приложение А).

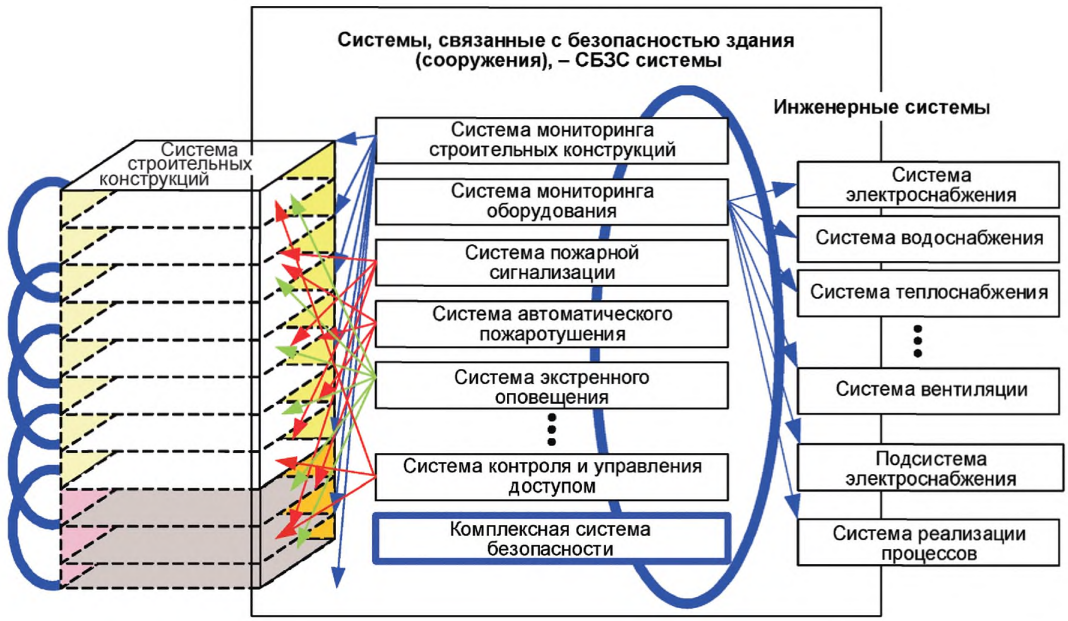


Рисунок 1 — Модель здания или сооружения как сложной системы

Эти элементы взаимосвязаны друг с другом и вместе действуют как единое целое, обеспечивая прочность и устойчивость системы строительных конструкций объекта к механическим нагрузкам и воздействиям.

5.2.2 Инженерные системы

5.2.2.1 В состав инженерных систем жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, поддержания комфорта здания или сооружения включают в различных сочетаниях системы, неполный перечень которых приведен в А.2 (приложение А).

5.2.2.2 Системы жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, поддержания комфорта устраивают таким образом, чтобы обеспечивалось выполнение назначенных функций, определенных в утвержденных в установленном порядке техническом задании, технических условиях (специальных технических условиях) и проектной документации на объект.

5.2.2.3 В каждой из инженерных систем и/или подсистем могут быть предусмотрены собственные средства и системы защиты, предохраняющие эксплуатирующий персонал и пользователей здания или сооружения от причинения им вреда и предупреждающие переход инженерных систем или подсистем в опасное состояние и создание опасных ситуаций.

5.2.3 Системы обеспечения безопасности

5.2.3.1 Для обеспечения безопасности зданий или сооружений в их состав включают в различных сочетаниях Э/Э/ПЭ СБЗС системы и подсистемы, снижающие риск причинения вреда и/или тяжесть последствий, неполный перечень которых приведен в А.3 (приложение А), а также могут быть включены связанные с безопасностью системы, основанные на неэлектрических технологиях, и прочие средства уменьшения риска.

Примечание — Приемлемый уровень безопасности продукции может быть достигнут путем применения мер по снижению риска причинения вреда на всех стадиях ее ЖЦ в соответствии с руководством ИСО/МЭК [5].

5.2.3.2 СБЗС системы и подсистемы совместно с прочими средствами уменьшения риска применяют для снижения остаточного риска, обусловленного поведением строительных конструкций и инженерных систем при опасных воздействиях природного, техногенного и антропогенного характера, до уровня приемлемого риска, установленного в утвержденных в установленном порядке задании на проектирование объекта и/или технических условиях (специальных технических условиях).

Примечание — Снижение риска до уровня приемлемого риска показано на рисунке 2.

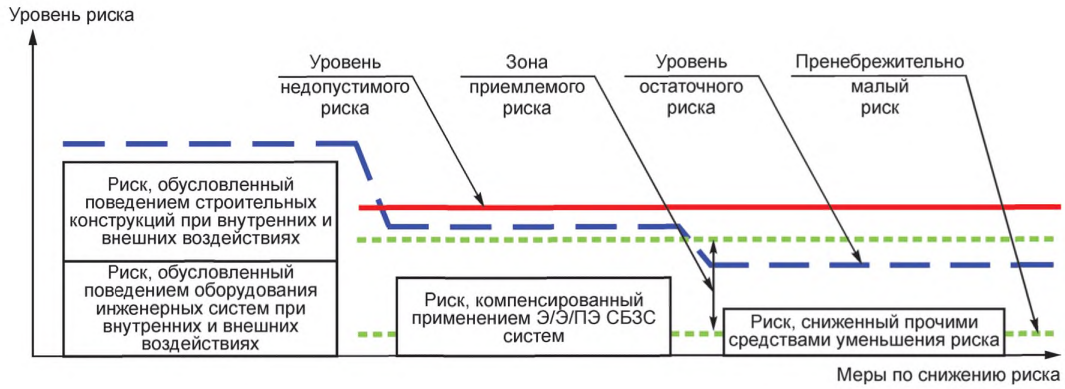


Рисунок 2 — Снижение риска до уровня приемлемого риска

5.2.3.3 Взаимодействующие Э/Э/ПЭ СБЗС системы и подсистемы проектируют и устраивают так, чтобы они обладали информационной совместимостью и поддерживали единые унифицированные протоколы обмена информацией.

5.2.3.4 Все СБЗС системы проектируют и реализуют (устанавливают и монтируют) на объекте таким образом, чтобы они надежно выполняли все предусмотренные для них функции безопасности в условиях взаимодействия этих систем и подсистем (смежных с ними систем и подсистем) между собой, при взаимовлиянии их друг на друга, в том числе с учетом электромагнитной совместимости, обеспечивая заданный уровень полноты безопасности.

5.2.3.5 Состав Э/Э/ПЭ СБЗС систем, применяемых в конкретных зданиях или сооружениях, определяют на стадии проектирования с учетом требований, установленных отдельными стандартами на эти системы.

5.3 Жизненные циклы систем

5.3.1 Полный жизненный цикл каждой Э/Э/ПЭ СБЗС системы и подсистемы охватывает стадии и этапы, приведенные в ГОСТ 34332.2 (раздел 7).

5.3.2 В рамках настоящего комплекса стандартов жизненный цикл Э/Э/ПЭ СБЗС систем рассматривают совместно с жизненным циклом здания (сооружения).

Примечание — За один жизненный цикл системы конструкций здания (сооружения) может проходить несколько жизненных циклов Э/Э/ПЭ СБЗС систем.

5.3.3 Общие требования к отдельным стадиям жизненного цикла Э/Э/ПЭ СБЗС систем устанавливают по ГОСТ 34332.2.

5.3.4 Требования к Э/Э/ПЭ СБЗС системам на стадиях разработки и реализации проекта, мерам по снижению рисков, методам оценки полноты безопасности и подтверждения соответствия устанавливают в стандарте на требования к системам.

5.3.5 Требования к программному обеспечению Э/Э/ПЭ СБЗС систем на стадии его разработки и реализации, методы достижения полноты безопасности и оценки соответствия устанавливают в стандарте на требования к программному обеспечению (ПО) этих систем.

5.3.6 Требования к прочим средствам уменьшения риска и системам мониторинга строительных конструкций и оборудования инженерных систем устанавливают в стандарте на системы мониторинга конструкций и прочие средства уменьшения риска.

5.3.7 На стадии эксплуатации в периодах технического обслуживания Э/Э/ПЭ СБЗС систем, их видоизменения (модификации), ремонта систем, в периодах ремонта объекта, должны быть предусмотрены дополнительные меры по поддержанию уровня безопасности объекта на приемлемом уровне.

6 Проектные опасности

6.1 Для каждого здания и сооружения на этапе разработки задания на проектирование должны быть установлены проектные опасности и угрозы, которые должны быть учтены при проектировании объекта и его систем.

6.2 Для особо опасных, технически сложных и уникальных объектов, объектов повышенного уровня ответственности, имеющих важное социальное, экономическое и оборонное значение, а также объектов в области гражданской обороны, разрабатывают технические условия (специальные технические условия), содержащие дополнительные требования, учитывающие антропогенные опасности, модели нарушителей, модели угроз, в том числе террористического характера, с учетом особенностей объекта и местных условий.

Примечание — Порядок разработки, получения и согласования таких технических условий (специальных технических условий) устанавливается уполномоченными органами исполнительной власти государства — члена Содружества.

6.3 Разработка Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска осуществляется разработчиком проектной документации с учетом проектных опасностей и угроз, установленных в техническом задании на проектирование и технических условиях или специальных технических условиях (при их наличии).

6.4 При разработке Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска учитывают назначение, функции, сложность объекта, уровень ответственности, конструктивные и архитектурно-планировочные решения, состав инженерных систем (см. приложение А), расположение на местности, местные условия, виды и характер опасностей (см. приложение Б), факторы риска (см. приложение В) и возможную тяжесть последствий при реализации опасных событий (см. приложение Г).

6.5 Для каждой проектной опасности на стадии проектирования должны быть разработаны варианты моделей развития опасных событий с учетом вида и характера каждой опасности, взаимосвязи опасностей разных видов и их совокупного проявления с учетом местных условий, в том числе с учетом моделей нарушителей и моделей угроз, а также порядок действий в случае этих опасностей.

7 Риск

7.1 Риск как функционал и приемлемый риск

7.1.1 Риск R_i, возникающий в результате реализации i-го опасного события, определяют как функционал f_i характеризующийся частотой или вероятностью реализации опасного события и тяжестью последствий этого события (тяжестью причинения вреда) на основе выражения:

$$R_i = f_i (F_i \times C_i),$$

где f_i — функционал;

F_i — частота или вероятность реализации i-го опасного события;

C_i — тяжесть последствий — тяжесть вреда, причиненного в результате реализации i-го опасного события.

Элементы риска следующие: риск, относящийся к рассматриваемой опасности, который является функцией степени тяжести вреда, причиной которого может быть рассматриваемая опасность, и частоты или вероятности причинения вреда, которые определяется наличием опасной ситуации, возникновением опасного события и возможностью избежать причинение вреда или ограничить вред.

7.1.2 При реализации нескольких опасных событий для определения суммарного риска следует учитывать их совокупность в соответствии с законами теории вероятности.

7.1.3 Цель определения приемлемого риска для конкретного опасного события состоит в установлении, что считается приемлемым по отношению к обоим элементам риска — вероятности причинения вреда и степени тяжести вреда (см. 7.1.1).

7.1.4 Приемлемый риск, связанный с эксплуатацией или использованием зданий или сооружений, пребыванием людей, нахождением имущества, животных и растений на этих объектах и прилегающих

территориях, устанавливают в целях обеспечения соблюдения требований технических регламентов Таможенного союза (ТР ТС) [2] — [4] (в части обеспечения безопасности объектов инфраструктур), а также технического регламента Евразийского экономического союза (ЕАЭС) [5] (после его вступления в силу).

7.1.5 Приемлемый риск устанавливают на основе:

- законодательства государства — члена Содружества в части установления допустимого риска.

Пример — Максимальный допустимый индивидуальный пожарный риск в Российской Федерации установлен Федеральным законом от 22.07.2008 № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» (статья 93). Его величина не должна превышать одну миллионную в год;

- условий договора (контракта) между инвестором (техническим заказчиком) и застройщиком или иными заинтересованными сторонами;
- результатов анализа опасностей, возможных опасных событий и их последствий, проведенного организацией-проектировщиком на стадии проектирования с использованием количественных и/или качественных методов, приведенных в приложениях Ж — М, применительно к конкретному объекту с учетом его особенностей и местных условий.

7.2 Порядок достижения приемлемого риска

7.2.1 Приемлемый риск достигают с помощью итерационного процесса оценки риска и снижения риска в соответствии с концепцией безопасности, установленной в [5]. Этот процесс продолжают до тех пор, пока риск не будет снижен до уровня приемлемого риска (рисунок 3).

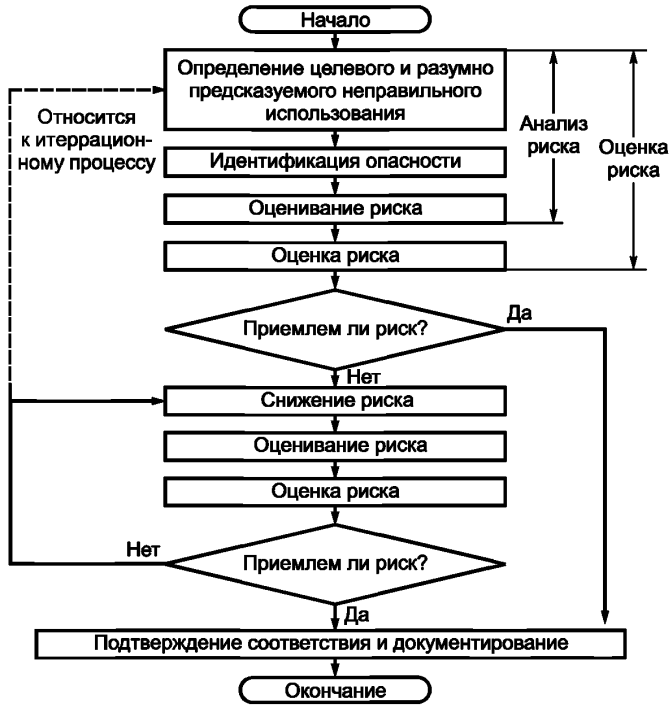


Рисунок 3 — Итерационный процесс оценки риска и снижения риска

7.2.2 Снижение риска осуществляют на стадиях проектирования, создания (строительства) и эксплуатации объекта и его систем (рисунок 4).

7.2.3 Для снижения риска до уровня приемлемого риска следует осуществить следующую последовательность действий:

- определить возможную группу или группы пользователей зданием или сооружением (включая рабочих, служащих; для жилых, общественных и многофункциональных зданий и сооружений — жильцов, посетителей, временно пребывающих лиц, в том числе уязвимые группы пользователей);

- определить группу или группы пользователей, персонала, эксплуатирующего здание и сооружение, и персонала, осуществляющего техническое обслуживание объекта, его систем и составляющих;

- определить использование по назначению и выявить возможное предсказуемое неправильное использование объекта и входящих в него систем, в том числе СБЗС систем;

- определить проектные опасности с учетом моделей опасностей, моделей угроз и моделей нарушителей;

- провести моделирование развития опасных событий с учетом их возможной взаимосвязи и взаимовлияния;

- выявить каждую опасность, включающую любую опасную ситуацию и опасное событие, предусмотренные техническими условиями (специальными техническими условиями) и/или заданием на проектирование, возникающие на всех этапах полного жизненного цикла СБЗС систем и их составляющих;

- оценить риск для каждой группы персонала, пользователей или контактирующей группы, возникающий вследствие определенной(ых) опасности(ей);

- определить, является ли риск приемлемым (например, по сравнению с рисками для подобных СБЗС систем, примененных ранее в подобных объектах при схожих условиях применения, или по сравнению с расчетными или целевыми значениями рисков);

- принять меры по снижению риска до уровня приемлемого риска, если риск окажется выше приемлемого риска.

7.2.4 Итерационный процесс анализа, оценки риска и снижения риска в соответствии с 7.2.3 (см. рисунок 3) следует применять на стадиях проектирования, создания (строительства) и эксплуатации объекта, его Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска (рисунок 4).

7.2.5 При выборе мер по снижению риска на стадиях проектирования, создания (строительства) и эксплуатации объекта и его систем (см. рисунок 4) следует руководствоваться следующими приоритетами:

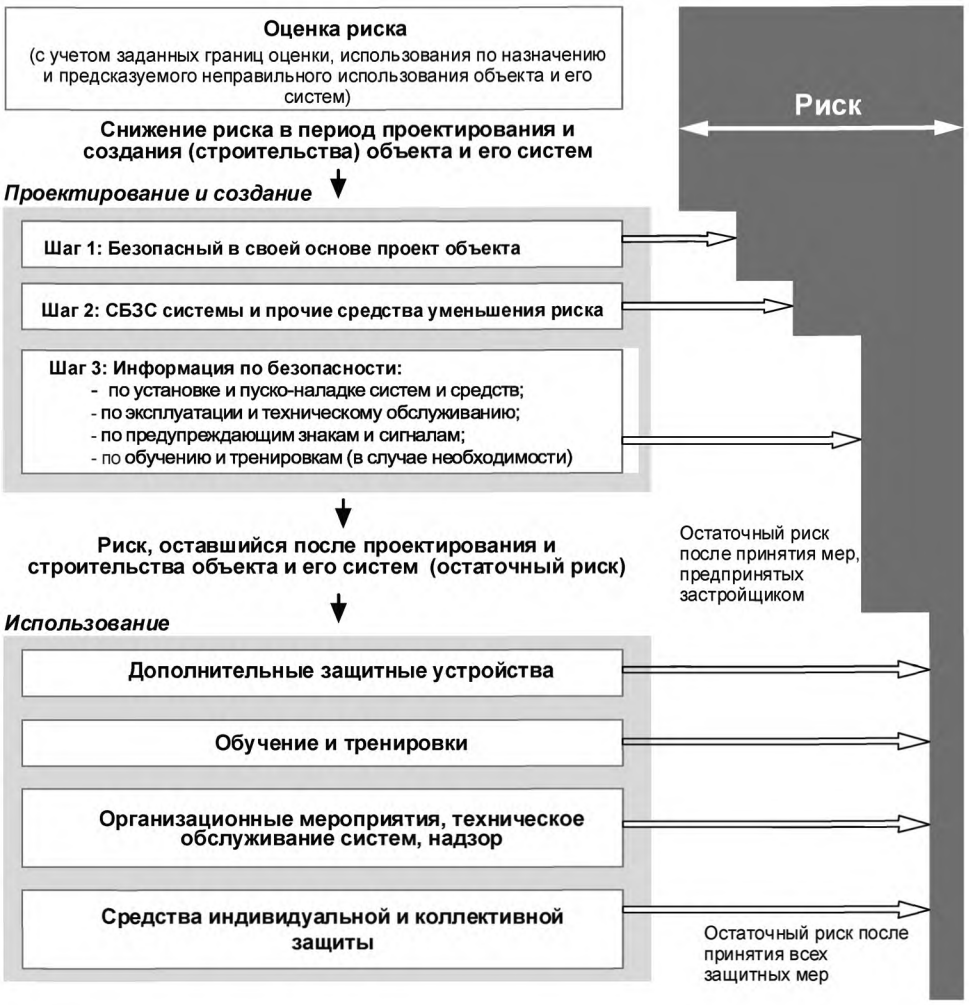


Рисунок 4 — Снижение риска на стадиях проектирования, создания (строительства) и эксплуатации объекта и его систем

- разработка проекта с эффективными решениями по безопасности;
- применение Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска;
- предоставление соответствующей информации строителям, пользователям, эксплуатирующему персоналу и лицам, осуществляющим техническое обслуживание систем.

Примечание — При проектировании Э/Э/ПЭ СБЗС систем в качестве начального риска (см. рисунок 4) может быть принят остаточный риск, оставшийся в результате принятых архитектурных, конструктивных и объемно-планировочных решений зданий и сооружений, утвержденных в установленном порядке.

7.2.6 На стадии проектирования расчет на возможное применение дополнительных защитных устройств, средств, систем, индивидуальных и коллективных средств защиты и предоставление информации пользователям, эксплуатирующему персоналу и персоналу, осуществляющему техническое обслуживание Э/Э/ПЭ СБЗС систем и их составляющих, не может служить основанием для снижения требований к качеству проекта.

Примечание — На стадиях проектирования и реализации проекта все работы, результаты которых могут оказать влияние на безопасность, следует осуществлять в соответствии с системами менеджмента качества, принятыми в организациях-исполнителях, не противоречащими требованиям ГОСТ ISO 9000 и ГОСТ ISO 9001.

7.2.7 Для снижения риска на стадии эксплуатации рекомендуется применять следующие меры (см. рисунок 4):

- применение дополнительных защитных систем и средств;
- обучение персонала, лиц, осуществляющих техническое обслуживание, и пользователей;

- осуществление организационных мероприятий, техническое обслуживание систем, надзор за безопасной эксплуатацией объекта и систем, безопасное пользование ими;
- применение средств индивидуальной и коллективной защиты.

Примечание — На этой стадии приоритеты в принятии мер по снижению риска могут отличаться от указанных в настоящем пункте. Они зависят от результатов реализации проекта и организации эксплуатации объекта, со всеми входящими в него системами, или его использования.

8 Принципы установления приемлемого риска

8.1 Уровень приемлемого риска, связанного с использованием и эксплуатацией здания или сооружения, устанавливают таким, чтобы обеспечивалось соблюдение требований соответствующего технического регламента, технических условий (специальных технических условий) и технического задания на проектирование объекта, утвержденных в установленном порядке.

8.2 При установлении уровня приемлемого риска должны быть приняты во внимание технические и технологические достижения, а также экономические и социальные факторы. Установление уровня приемлемого риска может быть основано на применении принципа разумной достаточности.

8.3 Установление приемлемого риска может быть осуществлено на основе принципов, приведенных в приложении Д.

9 Определение уровней полноты безопасности

9.1 УПБ Э/Э/ПЭ СБЗС систем должны быть определены на стадии проектирования.

9.2 При определении уровней функциональной безопасности Э/Э/ПЭ СБЗС систем должны быть учтены архитектурные, конструктивные, объемно-планировочные решения, а также уровни безопасности системы строительных конструкций и инженерных систем зданий и сооружений.

9.3 В зависимости от применяемых Э/Э/ПЭ СБЗС систем, новизны проекта, объема достоверных данных о свойствах систем и иных факторов для определения полноты функциональной безопасности этих систем могут быть применены количественные (приложение И) или качественные (приложения Ж, К—М) методы.

9.4 Для инженерных расчетов полноты безопасности Э/Э/ПЭ СБЗС систем следует применять стандартизованные или общепризнанные методы.

Приложение А
(справочное)

Системы

А.1 Система строительных конструкций

В систему строительных конструкций здания или сооружения входят в различных сочетаниях следующие элементы, влияющие на безопасность:

- фундамент;
- несущие и самонесущие стены (наружные, внутренние, противопожарные);
- колонны;
- наружные стены нижних этажей;
- стены, отделяющие помещения для систем управления объектом, инженерными системами жизнеобеспечения, системами обеспечения безопасности;
- стены лестничных клеток;
- перекрытия и элементы перекрытий (балки, ригели, рамы, фермы);
- ветровые связи;
- конструкции шахт и машинных отделений лифтов.

А.2 Инженерные системы

В состав инженерных систем жизнеобеспечения, систем и подсистем энерго-, ресурсосбережения, поддержания комфорта зданий и сооружений, а также реализации процессов входят следующие системы или подсистемы:

- водоснабжения;
- канализации;
- водостоков и дренажа;
- теплоснабжения;
- отопления;
- автономных источников теплоснабжения;
- тепловоздушных завес;
- приточно-вытяжной вентиляции;
- кондиционирования воздуха;
- холодоснабжения;
- вертикального транспорта;
- мусороудаления;
- пылеуборки;
- электроснабжения;
- электроосвещения;
- наружного освещения фасадов;
- учета потребления энергоресурсов;
- учета водопотребления;
- энергосбережения;
- диспетчеризации;
- автоматизированного управления зданием и сооружением;
- оперативной радиосвязи;
- телефонной связи общего пользования;
- телефонной связи УПАТС;
- диспетчерской (технологической) телефонной связи;
- домофонная (видеодомофонная) — в жилых зданиях;
- радиотрансляции;
- УКВ ЧМ/FM радиовещания (в жилых зданиях);
- широкополосная интерактивная система кабельного телевидения (в жилых и многофункциональных зданиях);
- спутникового телевидения (в жилых зданиях);
- местного проводного вещания;
- звукоусиления залов и помещений (в административных, общественных и многофункциональных зданиях);
- ларингофонная система — в зданиях учебных заведений;
- конференц-система — в административных, общественных, многофункциональных зданиях, зданиях учебных заведений и научных организаций;

- видеоконференц-система — в административных, общественных, многофункциональных зданиях, зданиях учебных заведений и научных организаций;
- видеопроекции — в административных, общественных, многофункциональных зданиях, зданиях учебных заведений и научных организаций;
- кинофикации — а в кинотеатрах, зрелищных, многофункциональных зданиях и сооружениях;
- перевода речи — в зданиях учебных заведений, научных организаций, многофункциональных зданиях;
- локальных вычислительных сетей;
- электрочасификации;
- управления товарооборотом — в торговых заведениях;
- управления гостиницей — в гостиницах;
- реализации производственных, технологических и иных процессов;
- звуковая студия — в зданиях учебных заведений, научных учреждений, объектах телерадиовещания;
- телевизионная студия — в зданиях учебных заведений, научных организаций, сооружениях телерадиовещания;
- видеостудия — в зданиях учебных заведений, научных учреждений, объектах телерадиовещания;
- пневмопочта;
- узел подключения внешних интегральных сетей — в жилых, административных, общественных зданиях, зданиях учебных заведений и научных организаций;
- структурированная кабельная сеть;
- интеграции подсистем.

А.3 Системы обеспечения безопасности

В состав систем обеспечения безопасности зданий и сооружений входят следующие Э/Э/ПЭ СБЗС системы или подсистемы:

- аварийного освещения;
- заградительных огней (для высотных объектов);
- автоматического пожаротушения;
- газового и порошкового пожаротушения;
- пожарной сигнализации;
- противодымной защиты;
- контроля тока утечки;
- контроля воздушно-газовой среды, в том числе:
  а) окиси углерода (CO),
  б) ядовитых паров и газов,
  в) взрывоопасных газов и паров,
  г) агрессивных паров и газов,
  д) взрывоопасной пылевоздушной смеси;
- контроля уровня жидкостей в емкостях и бассейнах;
- контроля сосудов под давлением;
- контроля биологической защиты;
- контроля радиации;
- мониторинга состояния конструкций и основания здания;
- мониторинга и аварийного управления автоматики систем безопасности;
- мониторинга и аварийного управления инженерными системами;
- охраны периметров;
- контроля и управления доступом;
- телевизионного наблюдения
- охранного освещения;
- эвакуационного освещения;
- охранной сигнализации;
- обнаружения людей;
- оповещения и управления эвакуацией людей;
- оперативной связи;
- защиты информации;
- структурированная кабельная сеть;
- интегрированная кабельная сеть безопасности;
- КСБ*.

* При объединении двух и более систем или подсистем.

Приложение Б
(справочное)

Источники, виды и характер опасностей

При рассмотрении СБЗС систем в зависимости от местных условий следует учитывать перечисленные ниже опасности.

Природные опасности:

- землетрясение — в сейсмоопасных зонах;
- сель — в селеопасных зонах;
- оползень, обвал — в зонах опасности оползней, обвалов;
- лавина — в лавиноопасных зонах;
- вулканическое извержение — в зонах вулканической деятельности;
- карст, суффозионный процесс — на территориях, подверженных карсту и суффозии;
- просадка в лессовых грунтах;
- наводнение, затопление — в зонах опасности наводнений и затоплений;
- подтопление;
- сильный ветер, шквал, шторм, смерч, ураган;
- гроза — в зонах повышенной грозовой активности;
- осадки;
- гололед — в зонах опасности обледенений;
- чрезмерно низкая или высокая температура среды — в отдельных климатических зонах.

Техногенные опасности:

- механическая опасность, например, нарушения прочности и устойчивости конструкций;
- опасность пожара;
- опасность взрыва — при наличии или образовании взрывоопасных веществ и материалов;
- промышленная опасность — для особо опасных промышленных объектов, процессов и технологий;
- термическая опасность — для объектов, где имеются высокотемпературные источники;
- химическая опасность — для химических производств, складов, хранилищ, объектов с большими массами химически активных веществ;
- электрическая опасность — для объектов, в которых используют электричество;
- опасность излучений — при наличии источников излучений;
- биологическая опасность — при наличии источников биологической опасности;
- ядерная опасность — для ядерных объектов, объектов производства, переработки и хранения ядерных материалов;
- радиационная опасность — для объектов, на территории которых имеются радиоактивные вещества и материалы.

Антропогенные опасности:

- вызванные прогнозируемым неправильным использованием систем и их составляющих:
  а) эксплуатирующим, обслуживающим персоналом различных групп,
  б) пользователями различных групп, включая уязвимую группу пользователей;
- вызванные злонамеренными действиями:
  а) криминального характера;
  б) террористического характера.

Приложение В
(справочное)

Факторы риска

При определении проектных опасностей учитывают указанные в таблице В.1 возможные взаимосвязанные источники опасностей и присущие им факторы риска.

Таблица В.1 — Опасности, источники и факторы риска

Наименование вида опасности	Фактор риска	Возможный источник
Механическая опасность	Физическое повреждение, травма, компрессионная асфиксия	Природный: землетрясение, оползни, сели, лавина, эрозия, обвал, ураган, наводнение. Техногенный: взрыв, авария, нарушение целостности конструкций, обрушение, затопление. Антропогенный: нападение, диверсия, терроризм
Опасность взрыва	Физическое повреждение, травма, ожог, компрессионная асфиксия	Природный: гроза, извержение вулкана. Техногенный: авария, пожар, взрыв. Антропогенный: поджог, осуществление взрыва, диверсии, инициирование аварии
Опасность пожара	Отравление продуктами горения, ожог, термическое повреждение, физическое повреждение, компрессионная асфиксия	Природный: гроза, извержение вулкана. Техногенный: взрыв, пожар, короткое замыкание в электрических цепях, перегрев электронагревательных приборов. Антропогенный: поджог, инициирование взрыва, аварии, нарушение правил пожарной безопасности
Термическая опасность	Термическое поражение	Природный: извержение вулкана. Техногенный: авария, нарушение технологического процесса (если процесс имеется) Антропогенные: инициирование аварии, диверсия
Опасность излучений (неионизирующих)	Поражение важных органов организма человека	Природный: солнечная радиация, извержение вулкана Техногенный: авария, нарушение технологического процесса, режима работы оборудования. Антропогенный: инициирование аварии, нарушение технологического процесса, режима работы оборудования
Биологическая опасность	Инфекционное заболевание	Природный: патогенные микроорганизмы, вирусы; грибки, плесень. Техногенный: нарушение режимов обращения, хранения, удаления, переработки биологических отходов; нарушение санитарных правил и норм. Антропогенный: распространение патогенных микроорганизмов и вирусов; нарушение санитарных правил и норм
Промышленная опасность	Физическое повреждение, травма, ожог, компрессионная асфиксия	Природный: отсутствует Техногенный: авария, нарушение технологического процесса, взрыв, пожар, подтопление. Антропогенный: осуществление взрыва, поджога, диверсии; нарушение правил эксплуатации, правил пожарной безопасности, взрывобезопасности, правил пользования системами жизнеобеспечения

Окончание таблицы В.1

Наименование вида опасности	Фактор риска	Возможный источник
Химическая опасность	Химическое поражение	Природный: выброс газа. Техногенный: взрыв, авария, утечка химически активных и ядовитых веществ. Антропогенный: осуществление взрыва, диверсии; нарушение правил эксплуатации систем жизнеобеспечения
Электрическая опасность	Поражение электрическим током	Природный: удар молнии. Техногенный: авария; нарушение работы электрооборудования; нарушение изоляции токонесущих цепей в результате взрыва, пожара, обрушения. Антропогенный: осуществление взрыва, диверсии, поджога; нарушение правил эксплуатации, правил электробезопасности, взрывобезопасности и пожарной безопасности
Радиационная опасность	Радиационное поражение организма человека	Природный: выброс радона. Техногенный: авария; нарушение режимов применения, обращения, хранения, транспортирования, переработки, захоронения радиоактивных веществ и материалов. Антропогенный: несанкционированное распространение радиоактивных веществ и материалов; нарушение правил обращения с радиоактивными веществами и материалами
Ядерная опасность	Радиационное поражение, термическое поражение, ожог, физическое повреждение	Природный: отсутствует. Техногенный: отсутствует. Антропогенный: маловероятен
Антропогенная опасность	Механическое, химическое, радиационное, биологическое повреждение (заболевание), травма, ожог, отравление продуктами горения	Природный: отсутствует. Техногенный: возможен в отсутствие систем, связанных с безопасностью инженерного оборудования. Антропогенный: нападение, диверсия, осуществление взрыва, поджога, инициирование аварии, распространение патогенных микроорганизмов и вирусов, ядовитых и радиоактивных веществ; нарушение правил эксплуатации, правил безопасности; ошибки операторов, ошибки пользователей

Приложение Г
(справочное)

Критерии и категории тяжести последствий

В качестве одного из критериев тяжести последствий при реализации опасных событий в здании или сооружении может быть выбран вред, причиненный жизни и здоровью людей, прибывающих на этих объектах и прилегающей к ним территории, и вероятный ущерб из-за гибели людей и причинения вреда их здоровью.

Возможная тяжесть последствий, основанная на этом критерии, приведена в таблице Г.1.

Таблица Г.1 — Возможная тяжесть последствий при реализации опасных событий

Категория тяжести последствий	Тяжесть последствий при реализации опасных событий на территории здания или сооружения и прилегающей территории	Вероятный ущерб из-за гибели людей, или причиненного вреда здоровью, млн. руб.
1	Ничтожные последствия	—
2	Причинение вреда здоровью одного человека	До 0,6
3	Причинение вреда здоровью от двух до десяти человек включ.	До 6
4	Гибель одного человека	До 17
5	Гибель двух и более человек	До 85
6	Гибель более десяти человек	До 460
7	Гибель более ста человек	До 12600

Приложение Д
(справочное)

Основные понятия риска и полноты безопасности

Д.1 Содержание приложения

В настоящем приложении содержится информация об основных понятиях риска и о связи риска с полнотой безопасности.

Д.2 Необходимое снижение риска

Необходимая степень снижения риска представляет собой такое снижение риска, которое должно быть обеспечено для достижения уровня риска, приемлемого в конкретной ситуации. Цель определения приемлемого риска для конкретного опасного события состоит в установлении величины «разумного» риска, учитывающего как частоту (или вероятность) возникновения опасных событий, так и их конкретные последствия. СБЗС системы предназначены для уменьшения частоты (или вероятности) опасных событий и/или тяжести последствий опасных событий. При определении приемлемого риска должно быть установлено требуемое снижение риска.

При определении приемлемого риска для конкретного применения учитывают:

- общие законодательные требования государства — участника Соглашения, законодательные требования, которые непосредственно относятся к конкретной области применения, руководящие указания исполнительных органов власти, осуществляющих регулирование в области безопасности;
- технические регламенты ТС и ЕАЭС;
- международные стандарты, межгосударственные стандарты и своды правил в конкретной области применения;
- договоры и соглашения между различными сторонами, участвующими в конкретной области применения;
- лучшие независимые промышленные, экспертные и научные рекомендации консультативных органов.

При определении требований к УПБ Э/Э/ПЭ СБЗС системы (систем) для достижения приемлемой частоты (вероятности) опасного события учитывают характеристики риска, существенные в конкретном применении, и ряд аспектов, приведенных ниже.

Д.3 Риски

Д.3.1 Индивидуальный риск

Для работников и членов общества обычно определяют разные целевые риски. Целевой индивидуальный риск для работников применим к человеку, наиболее подверженному опасности, и может быть выражен в общем (суммарном) риске в год, возникающем в течение его рабочей деятельности. Целевой риск применяют к гипотетическому человеку и, следовательно, учитывают процент времени нахождения человека на рабочем месте. Целевой риск применим ко всем рискам, которым подвержен человек, и для приемлемого риска в связи с конкретной функцией безопасности необходимо учитывать и другие риски.

Чтобы убедиться в том, что уровень общего риска уменьшен до уровня ниже заданного целевого риска, может быть применен подход, который заключается в выявлении и суммировании всех рисков для наиболее подверженного рискам человека. Такой метод может вызвать затруднения, если человек подвержен слишком многим рискам, а для разработки системы необходимы решения на ранних стадиях. Альтернативный подход состоит в распределении общего целевого индивидуального риска в процентном отношении между всеми рассматриваемыми функциями безопасности. Распределение процентов обычно можно осуществить, основываясь на опыте работы с ранее использованными методами.

При определении целевого риска для отдельной функции безопасности могут быть применены качественные методы, такие как графы риска, которые включают в себя оценку критических параметров, увеличивающих риски. Эти факторы являются следствием опасного события и его частоты. При их определении учитывают ряд параметров рисков: уязвимость при опасном событии, число людей, попадающих в область действия опасного события, вероятность того, что человек окажется там и тогда, где и когда происходит опасное событие (например, место пребывания людей) и возможность уклониться от опасного события.

При применении количественных методов обычно определяют, находится ли параметр в определенном диапазоне. При использовании таких методов и выборе критериев у разработчика должен быть высокий уровень уверенности в том, что целевые риски не превышены. Для обеспечения безопасности устанавливают границы диапазона для всех параметров таким образом, чтобы применение при граничных значениях всех параметров удовлетворяло заданным критериям риска. При таком подходе установления границ существует слишком мало приложений, в которых все параметры будут иметь наихудшие значения в своем диапазоне.

Если риску отказа Э/Э/ПЭ СБЗС систем подвергаются не работники, а обычные члены общества, то используют несколько меньшее значение целевого риска.

Д.3.2 Социальный риск

Социальный риск возникает, когда единичное событие влечет за собой многочисленные жертвы (см., например, строку 7 таблицы Г.1 приложения Г) и вызывает социально-политический отклик. Критерий социального риска обычно выражается как максимальная накопленная частота травм с летальным исходом определенного числа человек. Этот критерий обычно выражен одной или несколькими линиями на графике *F* от *N*, где *F* — кумулятивная частота опасностей, а *N* — число несчастных случаев с летальным исходом в результате опасных событий. В логарифмической шкале это соотношение обычно представляет собой прямую линию.

Д.3.3 Отдельные подробности риска

При выборе критерия риска, который будет применен к определенной угрозе, может понадобиться рассмотреть подробности риска на протяжении срока службы объекта или системы. Остаточный риск может варьироваться от низкого (непосредственно после контрольных проверок или текущего ремонта) до максимального (непосредственно перед контрольными проверками). Если промежутки времени между контрольными проверками значительные, предпочтительно указывать максимальную вероятность опасности непосредственно перед контрольной проверкой, или чтобы вероятность запросов к Э/Э/ПЭ СБЗС системе *PFD(t)* или частота запросов в час *PFH(t)* находились ниже верхней границы УПБ на большей части задаваемого интервала времени (например, на 90 %).

Д.3.4 Роль связанных с безопасностью систем

Э/Э/ПЭ СБЗС системы способствуют снижению риска для достижения приемлемого риска. Они реализуют функции безопасности, необходимые для достижения или поддержания безопасного состояния УО, и предназначены для достижения самостоятельно, либо с помощью СБЗС систем, основанных на неэлектрических технологиях, и прочих средств снижения риска необходимой полноты безопасности для требуемых функций безопасности.

Д.3.5 Полнота безопасности

Полнота безопасности определяется как вероятность успешного выполнения Э/Э/ПЭ СБЗС системой требуемых функций безопасности в конкретных условиях в конкретные интервалы времени (см. 3.32). Полнота безопасности относится к характеристикам, описывающим способность системы выполнять функции безопасности (функции безопасности должны быть определены в спецификации требований к функциям безопасности).

При рассмотрении полноты безопасности учитывают, что она состоит из следующих двух компонентов:

- полноты безопасности апаратных средств, которая связана со случайными опасными отказами АС (см. 3.33);

- систематической полноты безопасности, обусловленной систематическими отказами, относящимися к опасным отказам (см. 3.35).

Достижение заданного УПБ АС может быть установлено с разумной степенью точности. Требования могут быть распределены между подсистемами в соответствии с нормальным законом распределения для вероятностей совместных событий. Для достижения требуемой полноты безопасности АС может потребоваться использование избыточной структуры АС.

Средняя вероятность отказа из-за систематических отказов может быть оценена, однако данные об отказах, возникающих из-за конструктивных ошибок и отказов по общей причине, таковы, что распределение отказов между ними может быть трудно предсказать. Это приводит к увеличению неопределенности в расчетах вероятности отказа в конкретной ситуации (например, вероятности отказа конкретной СБ системы). Поэтому должно быть принято решение о выборе лучших мер для сведения к минимуму этой неопределенности. Следует учитывать, что меры, принятые для уменьшения вероятности случайных отказов АС, не обязательно приводят к снижению вероятности систематических отказов. Такие меры, как резервирование с организацией параллельных каналов с идентичными АС, которые являются эффективными для уменьшения частоты случайных отказов АС, мало полезны для уменьшения частоты таких систематических отказов, которые вызваны ошибками в ПО.

Д.3.6 Режимы работы и определение уровня полноты безопасности

Д.3.6.1 Рассматривают три режима работы Э/Э/ПЭ СБЗС системы в зависимости от частоты запросов к ней для реализации ее функции(ий) безопасности:

- режим с низкой частотой запросов (частота запросов менее чем один раз в год);
- режим с высокой частотой запросов (частота запросов равна или превышает один раз в год);
- режим с непрерывным запросом (запрос существует постоянно).

Д.3.6.2 Полнота безопасности и снижение риска в режиме с низкой частотой запросов

Требуемый УПБ Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска должен быть установлен таким, чтобы обеспечить:

- среднюю вероятность отказов по запросу систем, достаточную для того, чтобы частота опасных событий не превышала значение приемлемого риска;

- возможность системы так изменить последствия отказов, чтобы риск не превышал значение приемлемого риска.

Примечания

1 На рисунке Д.1 представлена обобщенная модель снижения риска (режим с низкой частотой запросов), иллюстрирующая общие принципы. Модель риска для конкретного применения может отличаться от модели, представленной на рисунке Д.1.

2 На рисунке Д.2 представлена связь понятий риска и полноты безопасности.

Общая модель предполагает следующее:
- имеется УО и система управления УО;
- существует связанный с процессом человеческий фактор;
- средства защиты включают в свой состав:
  а) Э/Э/ПЭ СБЗС системы,
  б) прочие средства уменьшения риска.

В число рисков, представленных на рисунках Д.1 и Д.2, входят:

- связанный с УО риск — риск наличия конкретного опасного события для УО. При этом учитывается наличие системы управления УО и человеческого фактора. При определении этого риска не учитывают никакие специальные средства защиты (см. 3.45);
- приемлемый риск — это риск, который считается приемлемым в данном контексте на основе принятой в обществе системы ценностей (см. 3.37);
- остаточный риск — это риск возникновения опасных событий, связанных с УО, системой управления УО, а также человеческим фактором; он остается после добавления Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска (см. 3.27).

Связанный с УО риск является функцией от риска, связанного с самим УО, но учитывающего также снижение риска, достигнутое благодаря применению системы управления УО. Чтобы избежать неоправданных требований к полноте безопасности основной системы управления УО, настоящий стандарт вводит ограничения на требования, установленные в ГОСТ 34332.2 (пункт 7.5.7).

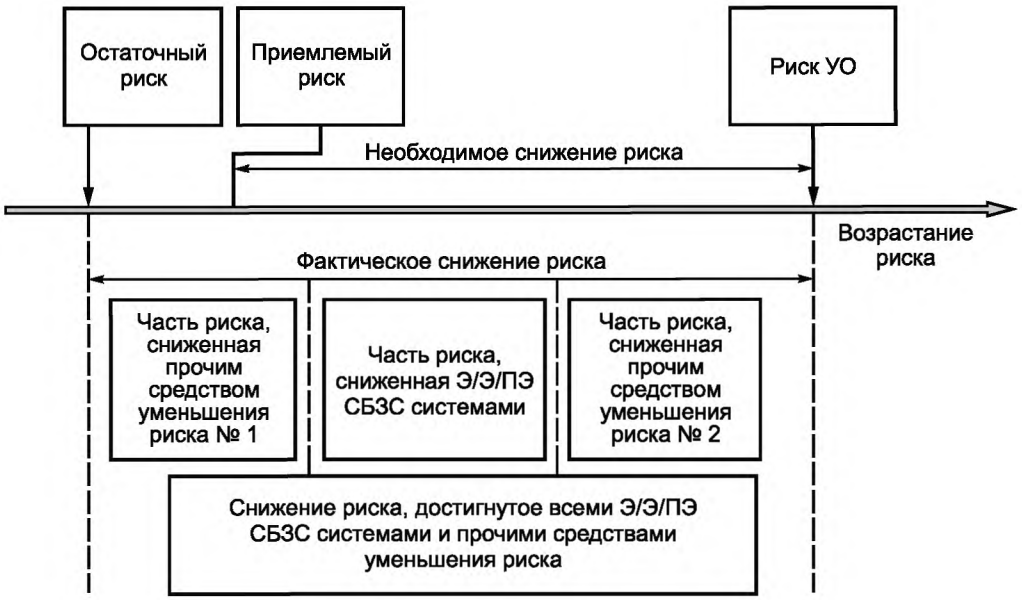


Рисунок Д.1 — Обобщенная модель снижения риска (режим с низкой частотой запросов)

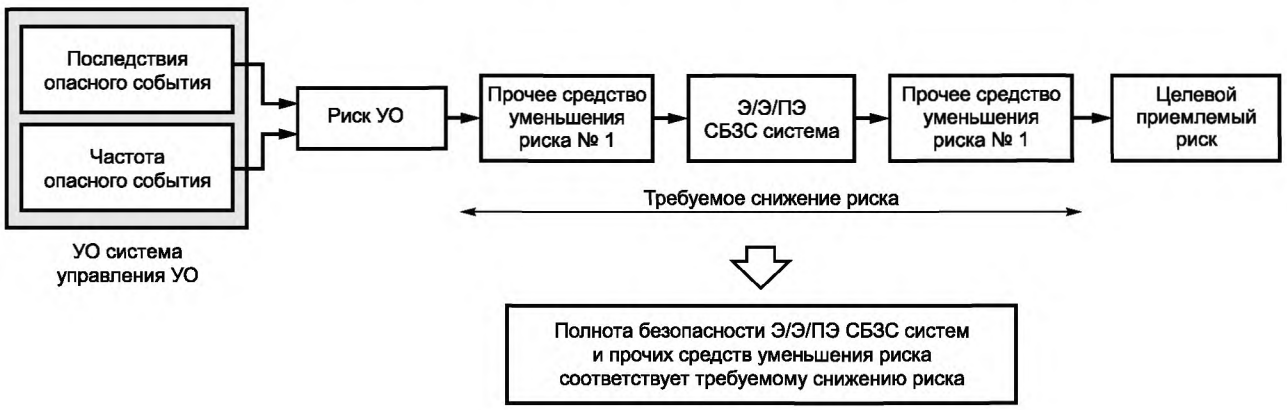


Рисунок Д.2 — Связь понятий риска и полноты безопасности

Необходимое снижение риска достигают комбинацией всех способов повышения безопасности. Модель процесса необходимого снижения риска от начального значения риска УО до конкретного приемлемого риска представлена на рисунке Д.1, который относится к функции безопасности, действующей в режиме с низкой частотой запросов.

Д.3.6.3 Полнота безопасности в режиме с высокой частотой запросов

Требуемый УПБ Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска должен быть установлен таким, чтобы обеспечить:

- среднюю частоту (интенсивность) отказов в час Э/Э/ПЭ СБЗС системы по запросу, достаточно низкую для того, чтобы частота опасных событий не превышала значения, соответствующего приемлемому риску;

На рисунке Д.3 представлена модель снижения риска при работе в режиме с высокой частотой запросов. В модели предполагается следующее:

- имеется УО и система управления УО;
- существует связанный с процессом человеческий фактор;
- средства обеспечения безопасности, включающие в свой состав:
  а) Э/Э/ПЭ СБЗС системы, работающие в режиме с высокой частотой запросов;
  б) прочие средства уменьшения риска.

К Э/Э/ПЭ СБЗС системе могут быть следующие запросы:

- общие запросы от УО;
- запросы, возникающие вследствие отказов системы управления УО;
- запросы, возникающие вследствие отказов по причине человеческого фактора.

Если общая частота (интенсивность) запросов, состоящая из всех запросов к системе, равна или превышает один раз в год, то критическим фактором является частота (интенсивность) опасных отказов Э/Э/ПЭ СБЗС системы. Систему проектируют и реализуют так, чтобы частота остаточных опасных событий никогда не превышала частоту (интенсивность) опасных отказов системы. Частота (интенсивность) может быть ниже, если прочие средства уменьшения риска снизят вероятность причинения вреда.

Д.3.6.4 Полнота безопасности для режима с непрерывным запросом

Требуемый УПБ Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска должен быть установлен таким, чтобы обеспечить среднюю частоту (интенсивность) опасных отказов в час Э/Э/ПЭ СБЗС системы, достаточно низкой для того, чтобы частота опасных событий не превышала значения, соответствующего приемлемому риску.

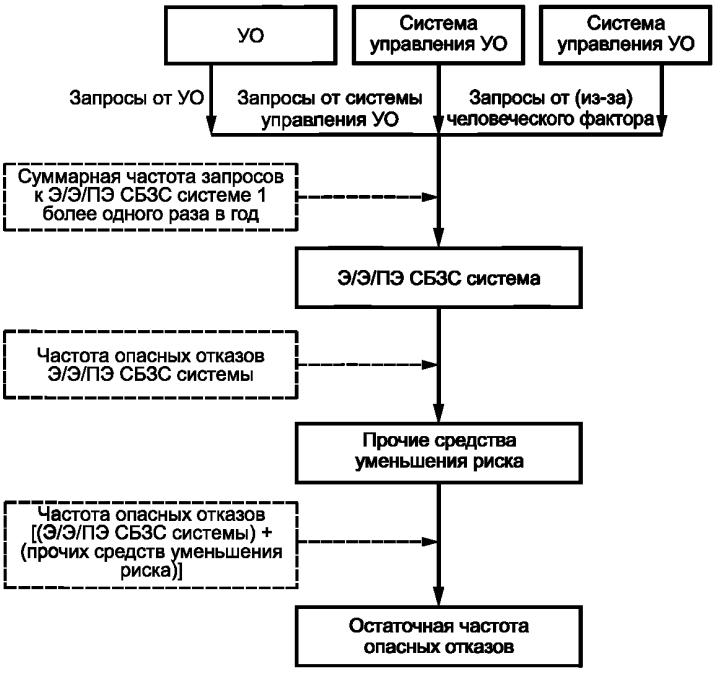


Рисунок Д.3 — Модель снижения риска при работе в режиме с высокой частотой запросов

Вместе с Э/Э/ПЭ СБЗС системой частоту остаточных опасных событий могут снизить прочие средства уменьшения риска, обеспечивая соответствующее снижение риска.

Модель снижения риска при работе в режиме с непрерывным запросом показана на рисунке Д.4.

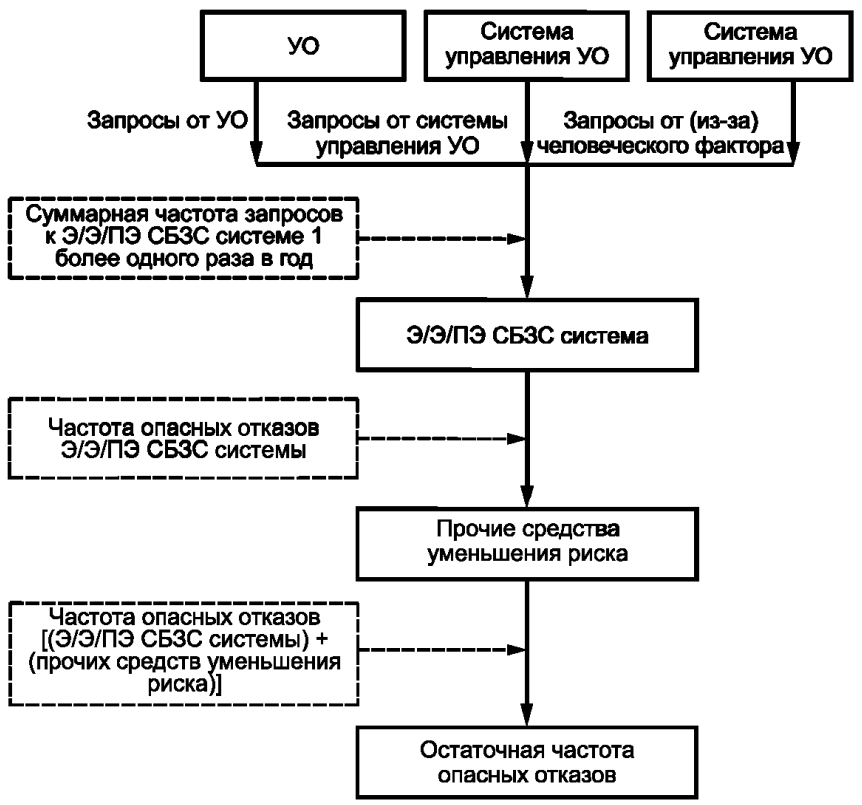


Рисунок Д.4 — Модель снижения риска при работе в режиме с непрерывным запросом

Д.3.6.5 Отказы по общей причине и зависимые отказы

При определении УПБ следует учитывать отказы по общей причине и зависимые отказы. Модели, показанные на рисунках Д.1 — Д.4, составлены в предположении, что каждая Э/Э/Э СБЗС система, противодействующая конкретной опасности, полностью независима. Во многих применениях такая независимость отсутствует. Например, в случаях:

- когда опасный отказ элемента в системе управления УО может вызвать запрос к Э/Э/ПЭ СБЗС системе, а в этой системе использован элемент, отказавший по той же причине. Например, если два датчика системы управления и Э/Э/ПЭ СБЗС системы разделены, но они оба могут отказать по общей причине.

Примечание — Иллюстрация отказов по общей причине элементов в системе представлена на рисунке Д.5;

- когда в каждой из нескольких Э/Э/ПЭ СБЗС систем применяют некоторое однотипное оборудование, каждое из которых отказало по общей причине (например, датчик одного и того же типа используют в двух отдельных Э/Э/ПЭ СБЗС системах, обеспечивающих снижение риска от одной и той же опасности).

Примечание — Модель отказов двух Э/Э/ПЭ СБЗС систем по общей причине представлена на рисунке Д.6;

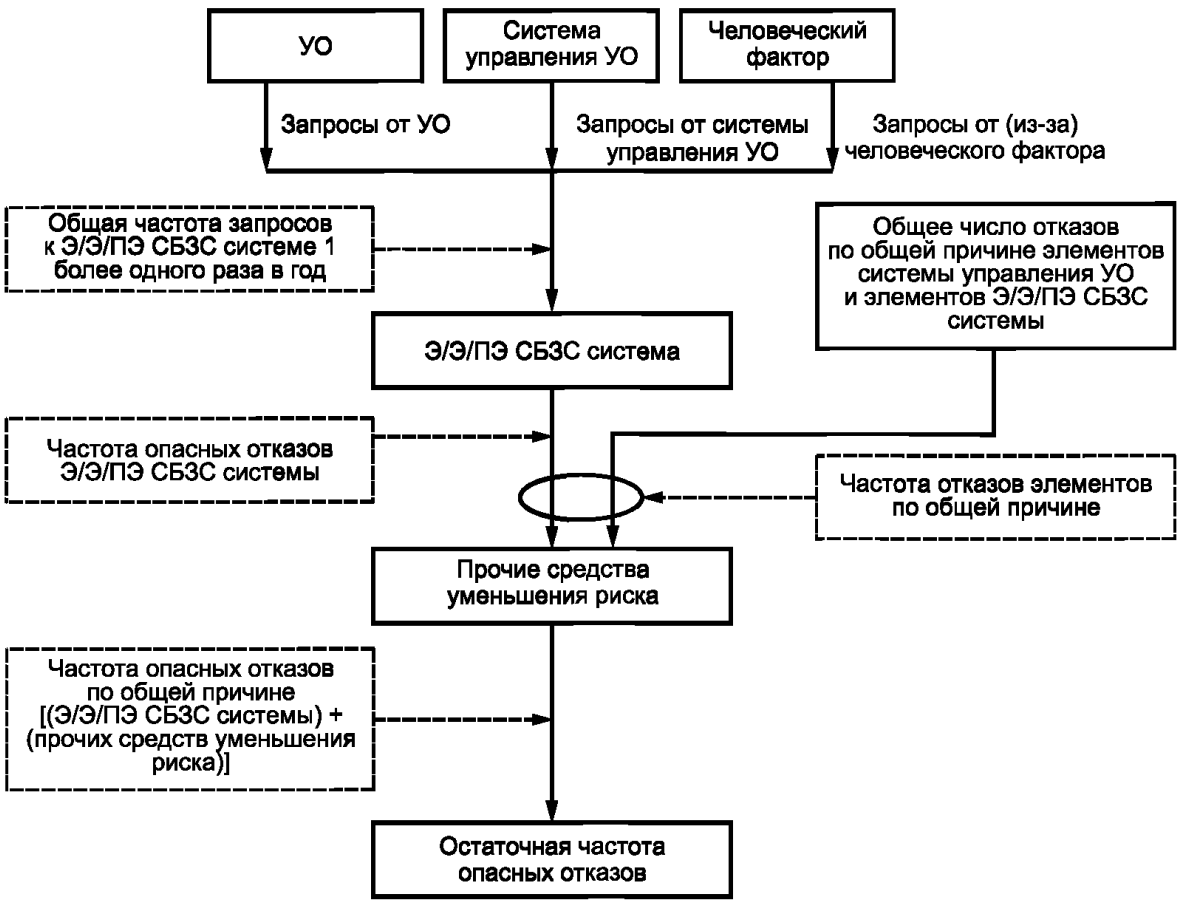


Рисунок Д.5 — Иллюстрация отказов элементов систем по общей причине

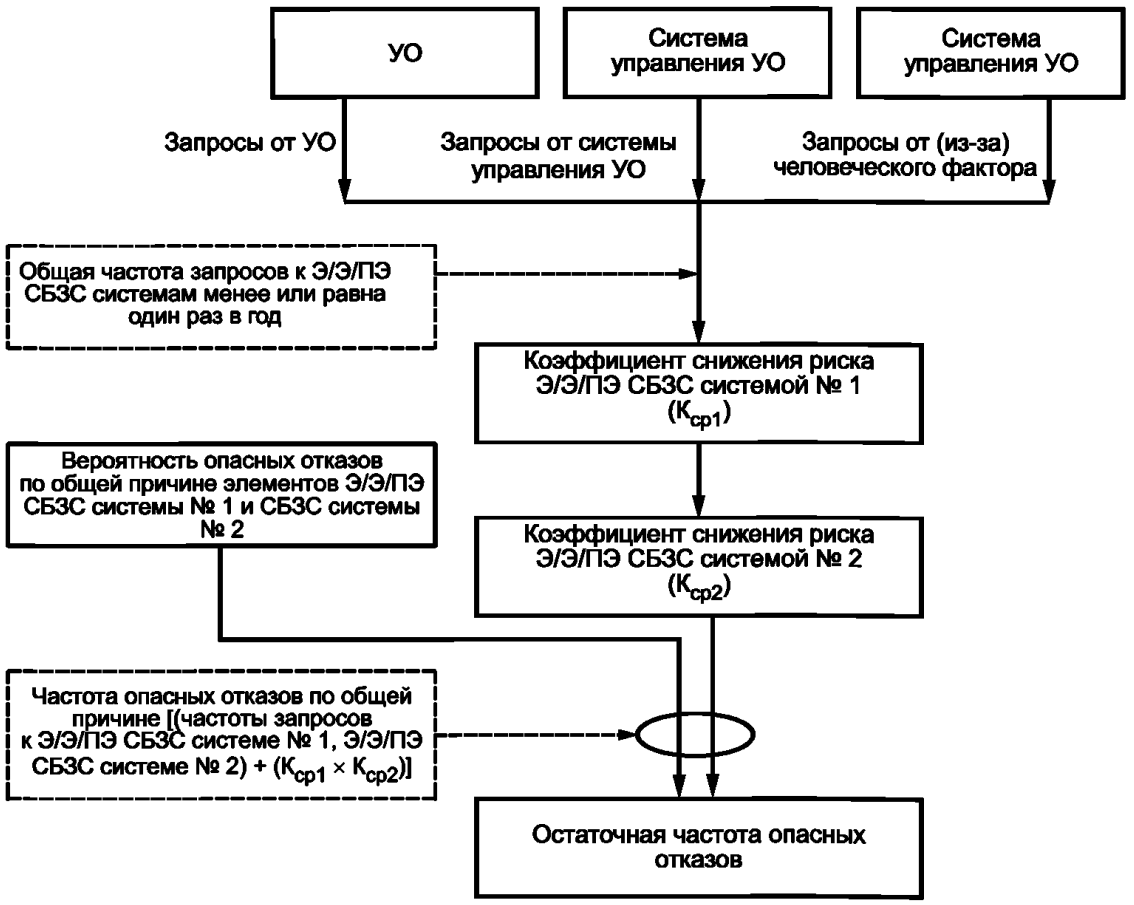


Рисунок Д.6 — Модель отказов двух Э/Э/ПЭ СБЗС систем по общей причине

- когда в нескольких различных используемых Э/Э/ПЭ СБЗС системах контрольные проверки проводят для всех систем одновременно. В таких случаях фактическая средняя вероятность опасных отказов по запросу, достигаемая комбинацией различных систем, будет значительно выше, чем средняя вероятность опасных отказов по запросу PFD_{avg}, получаемая умножением значений PFD_{avg} для отдельных систем;

- когда один и тот же конкретный элемент используют как в системе управления УО, так и в Э/Э/ПЭ СБЗС системе;

- когда в некотором количестве нескольких используемых Э/Э/ПЭ СБЗС систем применяют одинаковый элемент.

В таких случаях следует учитывать влияние отказов по общей причине. Необходимо рассмотреть, сможет ли окончательная структура системы соответствовать требуемой стойкости к систематическим отказам и требуемой вероятности случайных опасных отказов АС, связанных с общим необходимым снижением риска. Влияние отказа по общей причине сложно определить; обычно это требует построения специальных моделей (например, дерева отказов или модели Маркова).

Влияние общей причины будет более значимым в применениях с высокими УПБ. Для минимизации влияния общей причины в некоторых применениях может оказаться необходимым внести разнообразие в системы. При этом следует учитывать, что использование разнообразия может привести к трудностям на стадиях разработки, технического обслуживания и модификации Э/Э/ПЭ СБЗС систем. Внесение разнообразия может привести к ошибкам вследствие неосведомленности и недостатка опыта работы персонала с различными устройствами.

Д.3.6.6 Случай с несколькими слоями защиты

В случае применения нескольких слоев защиты (СЗ) для достижения приемлемого уровня риска могут возникнуть проблемы взаимодействия между системами, а также между системами и причинами запросов. Обычно существуют проблемы с нарушением синхронизации и отказами по общим причинам, и они могут быть значимыми факторами при высоких требованиях к общему снижению риска или низкой частоте запросов. Оценка взаимодействия между СЗ и между СЗ и причинами запросов может быть сложной и потребовать разработки целостной модели и основываться, например, на методе нисходящего проектирования с корневым событием в виде допустимой частоты опасных событий. Модель может включать в себя все слои безопасности для расчета фактического снижения риска и все причины запросов для расчета фактической частоты опасных событий. Это позволяет идентифицировать минимальные сечения (то есть сценарии отказа), определять слабые места (то есть кратчайшие минимальные сечения: единичные, двойные отказы и т. д.) в структуре систем и способствовать улучшению системы с помощью анализа чувствительности к опасным событиям.

Д.4 Риск и полнота безопасности

Важно учитывать различие между риском и полнотой безопасности. Риск — это мера частоты появления и последствий конкретного опасного события. Его можно оценить для различных ситуаций [риск УО, требуемое снижение риска для достижения приемлемого риска, фактический риск (см. рисунок Д.1)]. Понятие приемлемого риска определяют путем рассмотрения вопросов, описанных в Д.2. Полнота безопасности применима только к Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска. Полнота безопасности представляет собой меру вероятности того, что рассматриваемые системы/средства успешно обеспечат требуемое снижение риска для заданных функций безопасности.

Только после того, как допустимый риск установлен и получена оценка величины необходимого снижения риска, можно определить требования к полноте безопасности Э/Э/ПЭ СБЗС систем.

Примечание — Такая процедура может носить итерационный характер, что позволит осуществить оптимизацию разработки с целью выполнения различных требований.

Д.5 Уровень полноты безопасности и стойкость к систематическим отказам программного обеспечения

Для достижения Э/Э/ПЭ СБЗС системами необходимого снижения широкого диапазона риска важно иметь несколько доступных УПБ как способа удовлетворения требованиям полноты безопасности функций безопасности в системе. В качестве основы определения требований к полноте безопасности функций безопасности, частично реализованных связанным с безопасностью ПО, используют стойкость к систематическим отказам ПО. В спецификации требований к полноте безопасности должны быть указаны УПБ для Э/Э/ПЭ СБЗС систем.

В настоящем комплексе стандартов определены четыре УПБ. Наивысшим является уровень УПБ 4, наиболее низким — уровень УПБ 1.

Целевые значения интенсивности отказов для четырех УПБ установлены в ГОСТ 34332.2 (таблицы 1 и 2) для Э/Э/ПЭ СБЗС систем, работающих в режиме с низкой частотой (интенсивностью) запросов и для Э/Э/ПЭ СБЗС систем, работающих в режиме с высокой интенсивностью запросов или в режиме с непрерывным запросом.

Примечание — Для СБЗС систем, работающих в режиме с низкой частотой запросов, в качестве меры полноты безопасности применяют среднюю вероятность отказов выполнения функций безопасности по запросам. Для систем, действующих в режиме высокой частоты запросов, или с непрерывным запросом, в качестве меры полноты безопасности применяют среднюю частоту (интенсивность) отказов в час.

Д.6 Распределение требований безопасности

Распределение требований безопасности (требований к функциям безопасности и требований к полноте безопасности) по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска показано на рисунке Д.7, который идентичен рисунку 2, приведенному в ГОСТ 34332.2. Требования к стадии распределения требований безопасности установлены в ГОСТ 34332.2 (подраздел 7.6).

Примечания

1 Требования к полноте безопасности связывают с каждой функцией безопасности до распределения.

2 Функция безопасности может быть распределена по нескольким Э/Э/ПЭ СБЗС системам.

3 Методы, используемые для распределения требований полноты безопасности по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска, зависят, в первую очередь, от того, каким методом определена степень необходимого снижения риска — количественным или качественным (см. приложения Ж—М).

Д.7 Смягчающие системы

Смягчающие системы применяют в случае полного или частичного отказа других СБ систем, таких как Э/Э/ПЭ СБЗС системы. Цель применения — смягчение последствий, связанных с опасным событием, а не определением его частоты. Примером смягчающей системы является система автоматической пожарной сигнализации и автоматического пожаротушения (при обнаружении возгорания выполняются действия по тушению пожара).

При определении требований к полноте безопасности следует иметь в виду, что при обосновании тяжести последствий учитывают только дополнительные последствия. То есть необходимо определить увеличение тяжести последствий только за счет того, что рассматриваемая функция перестает выполняться. Это можно сделать, оценив сначала последствия в случае сбоев в работе системы, а затем рассмотрев, как изменяются последствия, если будет корректно работать ослабляющая функция. Если в системе происходят сбои, то последствий будет несколько, причем все они будут иметь различную вероятность. В этом случае может быть применен метод анализа дерева событий.

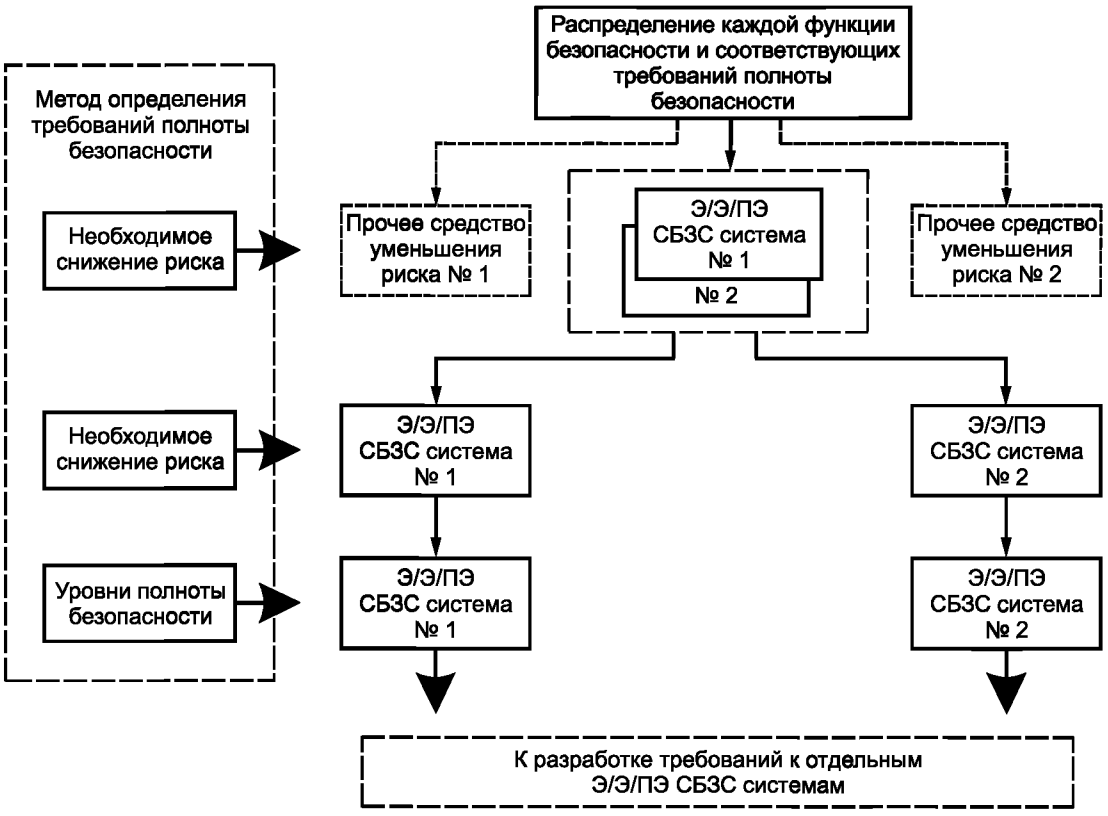


Рисунок Д.7 — Распределение требований безопасности по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска

Приложение Е
(справочное)

Выбор методов для определения требований к уровню полноты безопасности

Е.1 Общие положения

В настоящем приложении рассматривается ряд методов, которые могут быть применены при определении УПБ. Ни один из методов не является универсальным и не может быть использован как единственный для всех применений и пользователей методов. Пользователю необходимо выбрать наиболее подходящий или их комбинацию. При выборе наиболее подходящего метода следует рассмотреть следующие факторы:

- критерии приемлемого риска, которые должны быть выполнены (если требуется продемонстрировать, что риск снижен настолько, насколько это практически достаточно, то некоторые из методов не будут пригодны);
- режим действия функции безопасности (некоторые методы подходят только для режима с низкой частотой запросов);
- знания и опыт сотрудников, определяющих УПБ, а также владеющих традиционным подходом в данной области;
- степень уверенности в том, что полученный в результате остаточный риск удовлетворяет критериям, установленным организацией-пользователем (одни методы связаны с количественными целевыми показателями, в то время как другие методы являются только качественными);
- возможность применения нескольких методов (для предварительной оценки может быть использован один метод, а в случае выявления необходимости более строгого подхода для достижения более высокого УПБ может быть применен другой метод);
- тяжесть последствий (для последствий с многочисленными летальными исходами должны быть выбраны более строгие методы);
- возникают ли отказы с общей причиной для двух или нескольких Э/Э/ПЭ СБЗС систем, для Э/Э/ПЭ СБЗС системы и источника запросов.

Какой бы метод ни был использован, все предположения должны быть документально оформлены для дальнейшего управления безопасностью. Все решения должны быть документально оформлены для обеспечения возможности подтверждения УПБ и независимой оценки функциональной безопасности.

Е.2 Принцип разумной достаточности

Принцип «разумной достаточности»*, описанный в приложении Ж, может быть использован самостоятельно или в сочетании с другими методами для определения требований УПБ для функции безопасности. Его применение позволяет реализовать качественный и количественный подходы. При этом следует учитывать границу между уровнем неприемлемого риска и диапазоном разумной достаточности.

Е.3 Количественный метод определения уровня полноты безопасности

Количественный метод описан в приложении М. Он может быть использован совместно с принципом разумной достаточности (именуемым также ALARP), описанным в приложении Ж.

Количественный метод может быть использован как в простых, так и в сложных случаях. В сложных случаях для отображения модели опасности может быть построено дерево ошибок. Конечным событием, как правило, является один или несколько случаев с летальным исходом, и логическая схема, построенная для представления запросов и причин отказов Э/Э/ПЭ СБЗС систем, приведет к начальному событию. Если для реализации функций управления и функций защиты используют один и тот же тип оборудования, то для моделирования отказов с общей причиной применяют программные средства. В некоторых сложных случаях единичный отказ может произойти в более чем одном месте на дереве ошибок, и это потребует проведения логического упрощения с применением булевых методов. Эти инструменты также способствуют анализу чувствительности, который позволяет выявить главные факторы, влияющие на частоту конечного события. УПБ может быть установлен путем определения требуемого снижения риска для достижения критериев приемлемого риска.

Этот метод подходит для функций безопасности, действующих в режиме с непрерывным запросом или режиме с высокой частотой запросов и в режиме с низкой частотой запросов. Применение метода обычно приводит к низким УПБ, поскольку модель риска специально разработана для каждого применения, и для представления каждого фактора риска используют числовые значения, а не числовые диапазоны, используемые в калиброванных графах риска. Однако количественные методы требуют построения специальной модели для каждого опасного события. Моделирование требует навыков, инструментов и знаний в области применения, а также может занять значительное время на разработку и проверку модели.

---

* В международной практике именуемый «ALARP» — от английского «as low as reasonably practicable» — настолько низкий, насколько практически целесообразно (в отношении риска).

Е.4 Метод графа рисков

В настоящем подразделе описан качественный метод графа рисков. Этот метод позволяет определить УПБ, основываясь на знании факторов риска, связанного с УО и системой управления УО. При его использовании вводят несколько параметров, которые вместе описывают природу опасной ситуации при отказе СБ систем или при их недоступности. Из каждого из четырех наборов выбирают один параметр; выбранные параметры затем объединяют для принятия решения об УПБ, распределенном по функциям безопасности. Этот метод широко используют в машиностроении.

Представленный метод позволяет продемонстрировать, что риск был снижен до практически осуществимого низкого уровня. Это можно сделать, рассматривая возможности дальнейшего снижения риска, включая в модель дерева ошибок для каждой возможности дополнительные средства и затем, определив полученное снижение риска, сопоставить его со стоимостью реализации каждой такой возможности.

Настоящий метод может быть качественным. В этом случае выбор параметров носит субъективный характер и требует существенного анализа. Остаточный риск не может быть рассчитан из знания значений параметров. Он не применим, если организации требуется уверенность в том, что риск снижен до заданного числового значения.

Числовые значения параметров можно получить с помощью калибровки графа рисков по числовым критериям приемлемости риска. Зная числовые значения каждого параметра, можно получить числовое значение остаточного риска. Опыт показывает, что использование метода калибровки графа рисков может привести к высокому УПБ. Причина состоит в том, что калибровку обычно проводят с использованием наихудших значений по каждому параметру. Каждый параметр имеет диапазон в один десятичный порядок, поэтому в случаях, когда все параметры — средние для диапазона, УПБ будет на единицу выше, чем необходимо для приемлемого риска. Этот метод широко используют для процессов и в секторе морского судоходства.

В методе графа рисков среди причин запросов и причин отказов Э/Э/ПЭ СБЗС системы не учитывают отказы с общей причиной или вопросы, связанные с общей причиной для других СЗ.

Е.5 Анализ слоя защиты

Основной подход метода анализа слоя защиты (АСЗ) применяют в разнообразных модификациях. В приложении Л описано применение этого метода для определения УПБ.

Этот метод является количественным и при его применении необходимо определить допустимые частоты и тяжести последствий для каждого слоя.

СЗ, снижающим частоту причин отдельных запросов, задают числовое значение такого снижения. Не все СЗ связаны со всеми причинам запросов, поэтому рассматриваемый метод может быть применен в более сложных случаях. Числовые значения, задаваемые СЗ, могут быть округлены в большую сторону до следующей значащей цифры или следующего значащего десятичного значения. Если числовые значения СЗ округлены до следующей значащей цифры, метод в среднем дает более низкие значения требований по снижению риска и более низкие значения УПБ, чем калиброванные графы рисков.

Так как задаваемым величинам тяжести последствий для СЗ задают числовые целевые значения, пользователь метода может быть уверен, что остаточный риск удовлетворяет заданным критериям.

Описанный метод не применим для функций, действующих в режиме с непрерывным запросом, и не учитывает отказов по общей причине для причин запросов и Э/Э/ПЭ СБЗС систем. Однако данный метод можно скорректировать для таких случаев.

Е.6 Матрица тяжести последствий опасных событий

Метод оценки тяжести последствий опасных событий описан в приложении М. Неотъемлемым допущением в этом методе является условие, что добавление СЗ должно обеспечить снижение значения риска на один порядок. Следующее допущение состоит в том, что СЗ независимы от причины запросов и друг от друга. Описанный метод не применим для функций, действующих в режиме с непрерывным запросом. Метод может быть качественным; в этом случае выбор факторов риска субъективен и требует серьезного обоснования.

Остаточный риск нельзя рассчитать, зная выбранные факторы риска. Метод не применим, если пользователю метода требуется уверенность, что остаточный риск снижен до указанного числового значения.

Приложение Ж
(справочное)

Принцип разумной достаточности и концепция приемлемого риска

Ж.1 Общие положения

В настоящем приложении рассматриваются основные принципы одного из подходов к достижению допустимого риска. Подход включает в себя процесс постоянного улучшения, где все возможности, которые позволяют снизить риски, впоследствии анализируют с точки зрения их преимуществ и затрат.

Ж.2 Принцип разумной достаточности

Ж.2.1 Основные положения

Принцип, описанный в настоящем разделе, основан на результатах анализа, применяемого при управлении промышленными процессами, которые определенно показывает одно из тех:

- риск настолько велик, что он должен быть признан полностью неприемлемым;
- риск является (или может быть) столь малым, что его можно считать незначительным;
- риск попадает в промежуток между двумя категориями, определенными в первых двух перечислениях, и уменьшается до самого низкого реального уровня с учетом полученных от этого выгод и с учетом затрат на любое дальнейшее его снижение.

Принцип разумной достаточности (ALARP) показан на рисунке Ж.1. При этом принципе требуется, чтобы любой риск был уменьшен настолько, насколько это практически целесообразно. При выполнении этого условия результирующий риск считают приемлемым риском для конкретного применения.



Рисунок Ж.1 — Принцип разумной достаточности

Риск, превышающий определенный уровень, считают неприемлемым, и он не может быть оправдан при обычных обстоятельствах.

Ниже этого уровня находится область приемлемого риска, в которой деятельность может производиться при условии, что риски будут сделаны настолько малыми, насколько это практически достаточно.

Там, где риск является менее значительным, на его снижение потребуются меньшие затраты, и на другом краю области приемлемого риска баланс между затратами и выгодами может оказаться удовлетворительным.

Ниже области приемлемого риска уровни риска считаются настолько незначительными, что их дальнейшего снижения не требуется. Это область явной приемлемости, для которой риски являются малыми в сравнении с по-

вседневными рисками. В области явной приемлемости не требуется детальной проработки для демонстрации разумной достаточности; однако требуется сохранять бдительность для того, чтобы риск оставался на данном уровне.

Концепция разумной достаточности может быть использована тогда, когда приняты качественные или количественные целевые значения риска. В Ж.2.2 описан метод количественной оценки риска. В приложении И описан количественный метод, а в приложениях К—Н описаны качественные методы определения требуемого снижения риска для конкретной опасности. На этапе принятия решения в эти методы может быть включена концепция разумной достаточности.

Ж.2.2 Целевой приемлемый риск

Один из путей получения целевого приемлемого риска состоит в том, что для ряда последствий, которые должны быть определены, назначают допустимые для них частоты. Такое согласование последствий и допустимых частот достигается обсуждением и выработкой соглашения между заинтересованными сторонами (например, органами, осуществляющими техническое регулирование в области безопасности, теми, чья деятельность является источником рисков, и теми, кто подвергается рискам).

Чтобы использовать принцип разумной достаточности, необходимо установить соответствие между последствиями риска причинения вреда и приемлемой частотой его возникновения, что может быть сделано, введением классов риска. В таблице Ж.1 в качестве примера приведены четыре класса (I, II, III, IV) для разных частот возникновения риска и разных вариантов его последствий. В таблице Ж.2 дана интерпретация каждого из классов риска на базе концепции разумной достаточности. Описание каждого из классов риска выполнено на основе рисунка Ж.1. Подразумевается, что риски, определенные внутри каждого из классов, — это риски, по отношению к которым уже приняты меры по их снижению.

На рисунке Ж.1 представлены следующие классы рисков:

- риск класса I находится в области неприемлемого риска;
- риски классов II и III в области разумной достаточности, причем риск класса II находится внутри области приемлемого риска;
- риск класса IV находится в области явно приемлемого риска.

Для каждой конкретной ситуации или для сравнимых областей применения может быть разработана таблица, аналогичная таблице Ж.1, учитывающая широкий диапазон социальных, политических и экономических факторов. Каждому последствию может быть поставлена в соответствие частота и, таким образом, таблица будет заполнена классами рисков. Например, «частое» в таблице Ж.1 может обозначать событие, которое будет встречаться постоянно, и частота которого может быть определена как превышающая 10 раз в год. Критическим последствием могла бы быть гибель одного человека и/или многочисленные серьезные повреждения нескольких людей, либо несколько профессиональных заболеваний (см. таблицу Ж.2).

Таблица Ж.1 — Пример классификации рисков опасных событий

Частота опасных событий	Класс риска последствий опасных событий			
	катастрофических	критических	небольших	несущественных
Частые	I	I	I	II
Возможные	I	I	II	III
Редкие	I	II	III	III
Отдельные	II	III	III	IV
Маловероятные	III	III	IV	IV
Невозможные	IV	IV	IV	IV
Примечание — Реальное заполнение таблицы классами рисков I, II, III и IV зависит от зоны рисков, от реальной частоты, вероятности их появления и т. п. Таблица служит примером того, как таблица должна заполняться, и не предназначена для прямого применения.				

Таблица Ж.2 — Возможная интерпретация последствий

Наименование последствий	Содержание последствий
Катастрофические	Гибель большого числа людей (до 100 человек)
Критические	Гибель одного человека и/или многочисленные серьезные повреждения или заболевание до 10 человек
Небольшие	Небольшая травма или заболевание одного человека
Несущественные	—

Приложение И
(справочное)

Определение уровня полноты безопасности. Количественный метод

И.1 Общие положения

В настоящем приложении описано, как могут быть определены УПБ с использованием количественного подхода, и показано, как может быть использована информация, содержащаяся в таблице Ж.1 и подобных ей таблицах. Количественный подход приобретает важное значение, когда:

- приемлемый риск должен быть описан количественно (например, что конкретное последствие опасного события не должно происходить с частотой, превышающей один случай за 10^4 лет);
- для УПБ в Э/ЭПЭ СБЗС системах определены количественные ориентиры в соответствии с ГОСТ 34332-2 (таблицы 1 и 2).

Настоящее приложение иллюстрирует основные принципы. Данный метод применим, в частности, когда используют модель риска, показанную на рисунках Д.1 и Д.2 (приложение Д).

И.2 Основной метод

Данную модель используют для иллюстрации основных принципов, показанных на рисунке Д.1 (приложение Д). Для каждой функции безопасности, которая должна быть реализована Э/Э/ПЭ СБЗС системой, следует выполнить следующие основные шаги:

- установить допустимый риск при помощи таблицы, подобной таблице Ж.1 (приложение Ж);
- установить связанный с УО риск;
- установить необходимое снижение риска для достижения приемлемого риска;
- распределить необходимое снижение риска между Э/Э/ПЭ СБЗС системами и прочими средствами уменьшения риска в соответствии с ГОСТ 34332.2 (подраздел 7.6).

Таблица Ж.1 (приложение Ж) содержит частоты возникновения риска и позволяет определить численное значение целевого приемлемого риска (Ft).

Частота, относящаяся к риску УО, включая систему управления УО, и вопросы, связанные с человеческим фактором, но без учета каких-либо мер защиты, может быть определена с использованием количественных методов оценки риска. Частота возникновения опасного события в отсутствие средств защиты $F_{пр}$ представляет собой один из двух компонентов риска УО; другим компонентом является последствие опасного события. Частота $F_{пр}$ может быть определена с помощью:

- анализа интенсивности отказов в схожих ситуациях;
- данных из соответствующих баз данных;
- расчетов с применением соответствующих методов прогноза.

Настоящий стандарт накладывает ограничения на минимальную интенсивность отказов, которая может быть предъявлена для системы управления УО. Если задано, что система управления УО имеет интенсивность отказов меньше минимальной, то система управления УО должна рассматриваться как система, связанная с безопасностью, и должна быть объектом всех требований к Э/Э/ПЭ системам, содержащихся в настоящем стандарте.

И.3 Пример расчетов

На рисунке И.1 представлено распределение полноты безопасности и пример расчета полноты безопасности для Э/Э/ПЭ СБЗС системы. Для этого примера средняя вероятность отказа по запросу PFD_{avg} Э/Э/ПЭ СБЗС системы, которая является целевой мерой отказов для систем, работающих в режиме с низкой интенсивностью запросов [см. ГОСТ 34332.2 (таблица 1)], определяется выражением

$$PFD_{avg} \le F_t / F_{пр},$$

где F_t — приемлемая частота опасных событий;

$F_{пр}$ — интенсивность запросов к Э/ЭПЭ СБЗС системе.

Определение $F_{пр}$ для УО является важным из-за связи с PFD_{avg} и, следовательно, с УПБ.

Шаги, которые должны быть выполнены при определении УПБ (когда последствие C остается неизменным), приведены ниже (они также показаны на рисунке И.1) для ситуации, при которой необходимое снижение риска целиком достигается за счет одиночной Э/Э/ПЭ СБЗС системы, которая должна снизить интенсивность возникновения опасностей как минимум с $F_{пр}$ до F_t:

- определить частотную составляющую риска УО без учета каких-либо средств защиты ($F_{пр}$);
- определить последствие C без учета каких-либо средств защиты;

- определить, используя таблицу Ж.1 (приложение Ж), достигается ли для частоты $F_{пр}$ и последствия С приемлемый уровень риска. Если при использовании таблицы Ж.1 (приложение Ж) получен класс риска I, то требуется дальнейшее снижение риска. Риски классов IV или III могут быть приемлемыми рисками. Риск класса II требует дальнейших исследований.

Примечание — Таблицу Ж.1 (приложение Ж) используют для того, чтобы проверить, нужны ли меры по дальнейшему снижению риска, поскольку может оказаться возможным достигнуть допустимого риска без применения каких-либо средств защиты;

- определить вероятность отказа Э/Э/ПЭ СБЗС системы (PFD_{avg}) при работе по запросу, состоящего в невозможности достичь требуемого снижения риска (ΔR). Для постоянного последствия в описанной конкретной ситуации $PFD_{avg} = (F_p / F_{пр}) = \Delta R$. Для $PFD_{avg} = (F_p / F_{пр})$ УПБ может быть использован из таблицы 1 ГОСТ 34332-2 (например, для $PFD_{avg} = 10^{-2} – 10^{-3}$ *УПБ* соответствует УПБ 2).

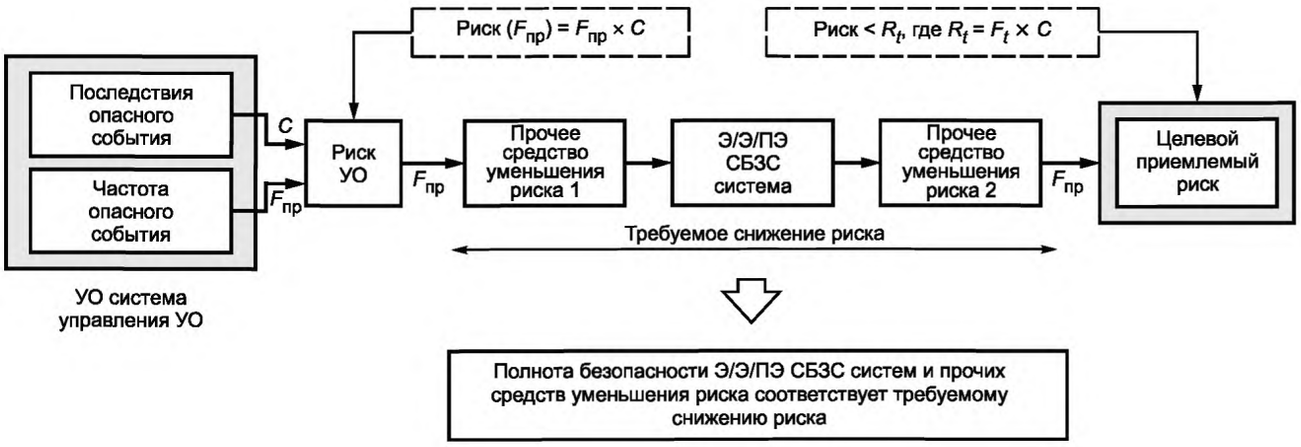


Рисунок И.1 — Распределение полноты безопасности и пример расчета полноты безопасности для Э/Э/ПЭ СБЗС системы

Эти шаги соответствуют случаю, когда все требуемое снижение риска достигается за счет одной СБЗС системы, которая должна уменьшить интенсивность возникновения опасностей как минимум с $F_{пр}$ до F_t.

Приложение К
(справочное)

Определение уровня полноты безопасности. Методы, основанные на графе рисков

К.1 Общие положения

В настоящем приложении описан метод графа рисков, который позволяет определить УПБ Э/Э/ПЭ СБЗС системы на основе знаний факторов риска, связанных с УО и системой управления УО. Он применим, в частности, когда модель риска соответствует модели, показанной на рисунках Д.1 и Д.2 (приложение Д). Этот метод может быть использован для получения как качественного, так и количественного результата.

При этом подходе в целях упрощения вводят ряд параметров, которые в совокупности описывают природу опасной ситуации, когда Э/Э/ПЭ СБЗС системы выходят из строя или недоступны. Из каждого из четырех наборов выбирают один параметр, и выбранные параметры затем объединяют для определения УПБ, относимого к функциям безопасности. Эти параметры:

- допускают содержательную градацию рисков, которые должны быть приняты;
- содержат ключевые факторы оценки риска.

К.2 Синтез графа рисков

Для синтеза графа рисков рассматривают риск R в отсутствие каких-либо Э/Э/ПЭ СБЗС систем. Ниже представлена упрощенная процедура, основанная на следующем уравнении:

$$R = \text{функция } (f) \text{ от заданного последствия } (C),$$

где f — частота опасного события в отсутствие каких-либо Э/Э/ПЭ СБЗС систем;

C — последствие опасного события (последствия могут быть связаны с причинением вреда жизни и здоровью людей или вреда имуществу, окружающей среде).

На частоту опасных событий f в данном случае влияют три фактора:

- частота и время нахождения в опасной зоне;
- возможность избежать опасного события;
- вероятность опасного события, которое происходит в отсутствие каких-либо Э/Э/ПЭ СБЗС систем (но, возможно, при наличии прочих средств уменьшения риска), которую называют вероятностью возникновения нежелательного события.

При этом получают следующие четыре параметра риска:

- параметр последствий опасного события (C);
- параметр частоты и продолжительности подвержения риску (F);
- параметр вероятности невозможности избежать риска (P);
- параметр вероятности возникновения нежелательного события (W).

Параметры риска могут быть определены качественно, как представлено в таблице К.1, или количественно, как представлено в таблице К.2. При определении числовых значений, связанных с каждым параметром в таблице К.2, потребуется процесс калибровки.

К.3 Калибровка

Цели процесса калибровки состоят:

- в описании всех параметров таким образом, чтобы группа, осуществляющая оценку УПБ, смогла выносить объективные суждения, основанные на основе объективных характеристик;
- в обеспечении УПБ, заданного для применения в соответствии с критериями корпоративного риска и учете рисков от других источников;
- в выборе параметра процесса, подлежащего верификации.

Калибровка графа риска — это процесс присвоения числовых значений параметрам графа риска. Калибровка формирует основу для оценки риска существующего процесса и позволяет определить требуемую полноту безопасности рассматриваемой системы.

Каждому из параметров присваивают диапазон значений таким образом, чтобы в случае комбинации средств градуированная оценка имеющегося риска осуществлялась в отсутствие конкретной функции безопасности. Таким образом определяют показатель степени доверия, чтобы отнести его к определенной функции безопасности. Граф риска связывает конкретные комбинации параметров риска с УПБ. Взаимосвязь между комбинациями параметров риска и УПБ устанавливают с учетом приемлемого риска, связанного с конкретными опасностями.

При рассмотрении рисков причинения вреда жизни и здоровью людей могут быть применены меры и требования, перечисленные в Д.2 (приложение Д), и методы, описанные в приложении Ж.

Если необходимо уменьшить частоту индивидуального риска до заданного максимума, трудно предположить, что необходимое снижение риска может быть достигнуто с помощью одной Э/Э/ПЭ СБЗС системы. Подверженные опасности лица подлежат широкому спектру рисков от разных источников (например, падение, пожар и взрыв). Во время калибровки трудно предусмотреть большое число опасностей, которым подвергаются люди в период опасного события.

При рассмотрении необходимого снижения риска может быть выбран критерий, связанный с дополнительными затратами на предотвращение событий с летальным исходом. Расчет может быть выполнен путем деления в годовом пересчете стоимости дополнительного оборудования и техники с более высокой стоимостью на возрастание снижения риска. Дополнительный УПБ обоснован, если дополнительные затраты на предотвращение летального исхода меньше, чем на заданную величину.

Перечисленные выше вопросы должны быть рассмотрены до указания каждого из значений параметров. Большинству параметров присваивают диапазон (например, если целевая частота запросов от конкретного процесса попадает в промежуток между оговоренным диапазоном и запросом в десять лет, то может быть использована величина W_3). Аналогичным образом требования в нижнем десятилетнем диапазоне W_2 могут быть применимы и для запросов в следующем более низком десятилетнем диапазоне W_1. Придание каждому параметру определенного диапазона помогает пользователю методом в принятии решений, на основе которых выбирают значение параметра для конкретного применения. Для калибровки графа рисков значения или диапазоны значений присваивают каждому параметру. Риск, связанный с каждой из комбинаций параметров, затем оценивают по определенным критериям риска.

Далее описания параметров изменяют таким образом, чтобы для всех комбинаций всех значений параметров достигались определенные критерии риска. В примере калибровки (как это показано в таблице К.2) вводят фактор «*D*» для того, чтобы диапазон требований, связанных с каждым фактором *W*, был модифицирован таким образом, чтобы достигался приемлемый риск. В некоторых случаях диапазоны, связанные с другими факторами риска, изменяют таким образом, чтобы отразить значения параметров, с которыми сталкиваются при распространении метода на другие применения. Калибровка представляет собой итерационный процесс и продолжается до тех пор, пока заданные критерии при емлемости риска не будут выполнены для всех комбинаций значений параметров.

Калибровку не следует выполнять каждый раз, когда УПБ должен быть определен для конкретного применения. Достаточно выполнить калибровку один раз для подобных опасностей. Регулировка может оказаться необходимой для конкретных проектов, если первоначальные предположения, сделанные в процессе калибровки, будут признаны недействительными для какого-либо конкретного проекта.

После определения параметров информация о том, каким образом были получены их значения, должна быть сохранена и доступна для проверки и последующего применения.

Важно, чтобы этот процесс калибровки был согласован в организации на высоком уровне с лицами, несущими ответственность за безопасность. Принятые решения определяют достигаемый общий уровень безопасности.

В графе риска сложно оценить возможность возникновения зависимого отказа между источниками запросов и оборудованием, используемым в Э/Э/ПЭ СБЗС системе. Поэтому возможна завышенная оценка эффективности Э/Э/ПЭ СБЗС системы. Если графы риска откалиброваны для частоты запросов выше одного раза в год, то требования к УПБ могут оказаться завышенными. В этом случае рекомендуется использовать другие методы.

К.4 Другие возможные параметры риска

Перечисленные выше параметры являются достаточно общими для того, чтобы можно было их распространить на широкий диапазон применений. Могут оказаться применения, для которых потребуется введение дополнительных параметров риска, например, при использовании новых технологий в УО и системах управления УО. Цель введения дополнительных параметров состоит в более точной оценке необходимого снижения риска [см. рисунок Д.1 (приложение Д)].

К.5 Реализация графа риска — общая схема

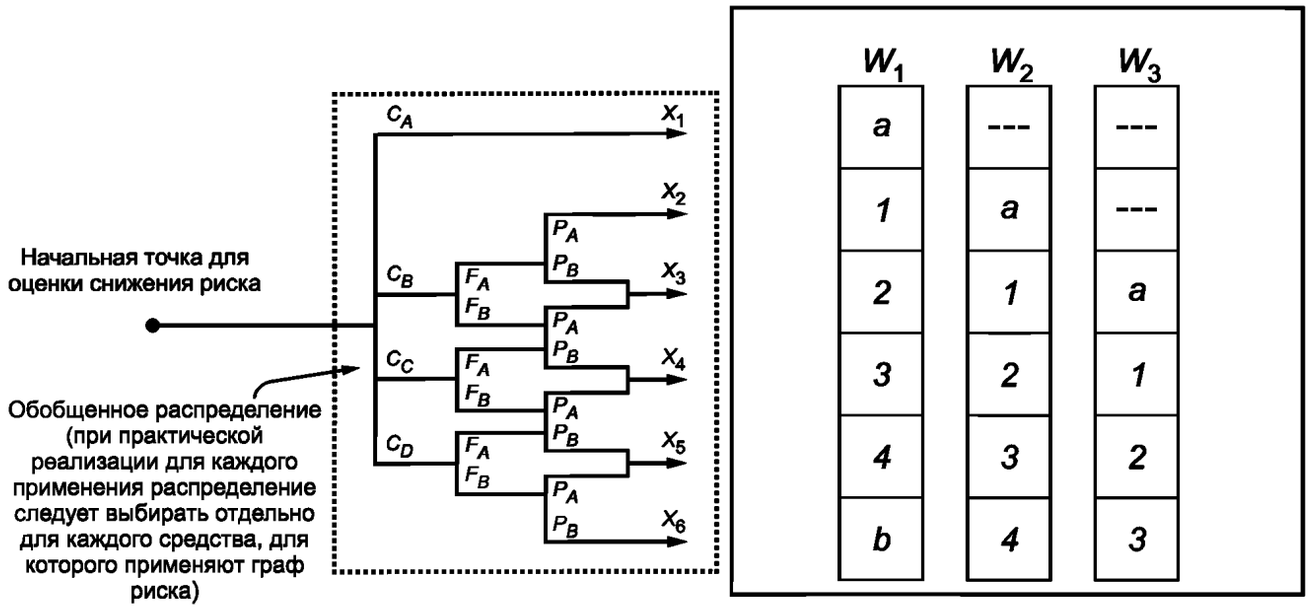
Общая схема графа рисков представлена на рисунке К.1. Для разработки графа рисков, аналогичного представленному на этом рисунке, используют комбинацию описанных выше параметров. Для этих параметров справедливы отношения:

$$C_a < C_b < C_c < C_d; F_a < F_b; P_a < P_b; W_1 < W_2 < W_3.$$

Пояснения к рисунку К.1 приведены ниже.

Использование параметров риска *C*, *F* и *P* приводит к ряду выходов X_1, X_2, X_3, ... X_n (точное число которых зависит от конкретной области применения, которая должна быть охвачена графом риска). На рисунке К.1 показана ситуация, при которой не применяют никаких дополнительных весовых параметров для более серьезных последствий опасных событий. Каждый из этих выходов отображают на одну из трех шкал параметров (W_1, W_2 и W_3). Каждая точка на этих шкалах является показателем необходимой полноты безопасности, которая должна выполняться

Э/Э/ПЭ СБЗС системой на стадии рассмотрения. На практике могут возникнуть ситуации, когда для определенных последствий применение одиночной Э/Э/ПЭ СБЗС системы не является достаточной мерой по снижению риска;



C — параметр последствий опасного события; *F* — параметр частоты и продолжительности подвержения риску; *P* — параметр вероятности невозможности избежать риска; *W* — вероятность возникновения нежелательного события; --- — требования безопасности отсутствуют; *a* — специальные требования безопасности отсутствуют; *b* — одиночная Э/Э/ПЭ СБЗС система недостаточна; 1, 2, 3, 4 — УПБ

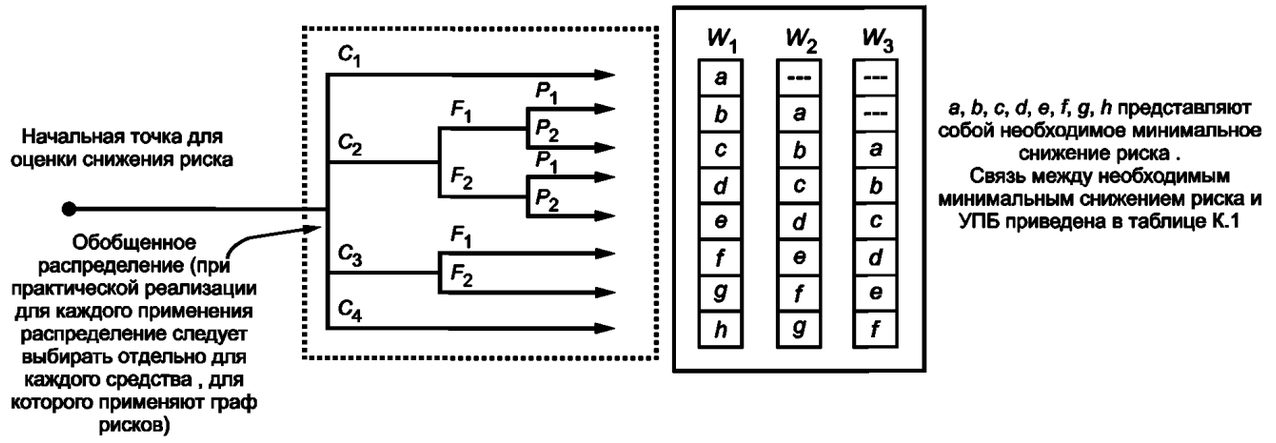
Рисунок К.1 — Общая схема графа рисков

Отображение на шкалах параметров W_1, W_2 или W_3 позволяет учесть вклад прочих средств уменьшения риска, которые должны быть использованы. Сдвиг значений параметров W_1, W_2, W_3 позволяет учесть вклад прочих средств уменьшения риска для трех уровней снижения риска. Шкала W_3 характеризует минимальное снижение риска с учетом вклада прочих средств уменьшения риска (т. е. при наибольшей вероятности возникновения нежелательного события), шкала W_2 — средний вклад и шкала W_1 — минимальный вклад. Для конкретного промежуточного выхода графа рисков (т. е. X_1, X_2 ... или X_6) и для конкретной шкалы параметров *W* (т.е. W_1, W_2 или W_3) окончательный выход графа риска дает УПБ Э/Э/ПЭ СБЗС системы (то есть УПБ 1, УПБ 2, УПБ 3 или УПБ 4) и является мерой необходимого снижения риска для данной системы. Это снижение риска, наряду с уменьшением риска, достигнутым применением других мер (например, с помощью СБЗС систем на основе неэлектрических технологий и прочих средств уменьшения риска), которое учитывают с помощью механизма шкалы *W*, определяет необходимое снижение риска для конкретной ситуации.

Параметры, обозначенные на рисунке К1 (C_a, C_b, C_c, C_d, F_a, F_b, P_a, P_b, W_1, W_2, W_3), и их веса должны быть точно определены для каждой конкретной ситуации или группы применений, либо объектов.

К.6 Пример графа рисков

Пример реализации графа рисков (иллюстрация общих принципов) с применением данных, представленных в таблице К.1, представлен на рисунке К.2. Использование параметров риска *C*, *F*, *P* приводит к одному из восьми выходов. Каждый из этих выходов отображают на одной из трех шкал (W_1, W_2 и W_3). Каждая точка на этих шкалах (*a*, *b*, *c*, *d*, *e*, *f*, *g* и *h*) является показателем необходимого снижения риска, который должен быть обеспечен Э/Э/ПЭ СБЗС системой.



C — параметр тяжести последствий; *F* — параметр частоты и продолжительности подвержения риску; *P* — параметр возможности избежать реализации опасного события; *W* — вероятность нежелательного события; *a*, *b*, *c*, ..., *h* — показатели необходимого минимального снижения риска для Э/Э/ПЭ СБЗС систем

Рисунок К.2 — Пример реализации графа рисков (иллюстрация общих принципов)

Таблица К.1 — Связь между необходимым минимальным снижением риска и УПБ

Необходимое минимальное снижение риска	УПБ
—	Требования безопасности отсутствуют
a	Специальные требования безопасности отсутствуют
b, c	1
d	2
e, f	3
g	4
h	Э/Э/ПЭ СБЗС система недостаточна

Пример данных, относящихся к графу рисков (см. рисунок К.2), приведен в таблице К.2.

Таблица К.2 — Пример данных, относящихся к графу рисков

Параметр риска		Классификация	Примечание
Последствия опасного события (*C*)	C_1 C_2 C_3 C_4	Небольшая травма. Серьезные травмы одному или нескольким лицам; гибель одного человека. Гибель нескольких людей. Гибель большого числа людей	1 Настоящая система классификации основана на учете риска причинения вреда людям. Для учета причинения вреда имуществу и окружающей среде должны быть разработаны другие классификации. 2 Для интерпретации C_1, C_2, C_3, C_4 следует учитывать последствия опасного события и последующее лечение
Частота и время пребывания в опасной зоне (*F*)	F_1 F_2	Редко более частое пребывание в опасной зоне. Часто постоянное пребывание в опасной зоне	3 См. примечание 1.

Окончание таблицы К.2

Параметр риска		Классификация	Примечание
Вероятность избегания опасности или опасного события (*P*)	P_1 P_2	Возможно при определенных условиях Практически невозможно	4 Для настоящего параметра принимают во внимание: - функционирование процесса [под наблюдением (т. е. управляется более опытным или менее опытным лицом) или без контроля]; - скорость развития опасного события (например, внезапно, быстро или медленно); - легкость распознавания опасности (например, видно сразу, обнаружение с помощью технических средств или обнаружение без технических средств); - избегание опасности, опасного события (например, возможно по путям эвакуации, не представляется возможным или возможно при определенных условиях); - фактический опыт обеспечения безопасности (такой опыт может быть с применением идентичного УО или подобного УО либо может отсутствовать)
Вероятность возникновения нежелательного события (*W*)	W_1 W_2 W_3	Очень небольшая вероятность того, что возникнет нежелательное событие, и вероятно возникновение только нескольких нежелательных событий. Небольшая вероятность того, что возникнет нежелательное событие, и вероятно возникновение только нескольких нежелательных событий. Относительно высокая вероятность того, что нежелательные события будут происходить и, скорее всего, часто	5 Целью фактора *W* является оценка частоты возникновения нежелательного события, которое происходит без добавления каких-либо СБЗС систем (Э/Э/ПЭ систем или систем на основе неэлектрических технологий), но при наличии прочих средств уменьшения риска. 6 Если недостаточен или полностью отсутствует опыт применения УО или системы управления УО, либо аналогичных УО и систем управления УО, то оценка параметра *W* может быть выполнена путем расчета. В этом случае расчет осуществляют по наихудшему сценарию

Пример калибровки графа рисков для общей схемы (см. рисунок К.1) приведен в таблице К.3.

Таблица К.3 — Пример калибровки графа рисков общего назначения

Параметр риска		Классификация	Комментарий
Последствия опасного события (*C*) Число погибших (оно может быть вычислено путем определения числа людей, отсутствующих в зоне, подвергающейся опасности, и умножения на уязвимость к идентифицированной опасности). Уязвимость определяется характером опасности, от которой необходима защита. Могут быть использованы следующие факторы: *V* = 0,01 — небольшой выброс токсичных или легковоспламеняющихся материалов; *V* = 0,1 — большая утечка горючего или токсичного материала; *V* = 0,5 — большая утечка горючего или токсичного материала и высокая вероятность возникновения пожара; *V* = 1 — разрыв оболочки или взрыв	C_A C_B C_C C_D	Небольшая травма Диапазон: св. 0,01 до 0,1. Диапазон: св. 0,1 до 1,0. Диапазон: св. 1,0	1 Система классификации основана на учете причинения вреда жизни и здоровью людей. 2 Для интерпретации C_A, C_B, C_C и C_D должны быть приняты во внимание последствия опасного события и последующее лечение

Окончание таблицы К.3

Параметр риска		Классификация	Комментарий
Последствия опасного события (*F*) Их вычисляют с учетом пропорциональной продолжительности времени, в течение которого зона пребывания людей подвергается опасности. Примечания 1 Если время пребывания в опасной зоне отличается от времени работы, то должно быть выбрано максимальное время. 2 Возможно использовать только F_a, если можно показать, что интенсивность запросов является случайной величиной и не имеет отношения к случаю, когда число пребывающих людей может быть больше, чем обычно. Последнее может быть при первом пуске оборудования или при расследовании нарушений	F_A F_B	Редко для более краткого пребывания в опасной зоне. Пребывание в опасной зоне менее 0,1. Часто для непрерывного пребывания в опасной зоне	3 См. комментарий 1
Вероятность избежать опасного события (*P*), если Э/Э/ПЭ СБЗС система не работает	P_A P_B	Принимают P_A, если выполнены все условия по пункту 4, указанные в колонке «Комментарий». Принимают P_B, если не все условия, перечисленные в колонке «Комментарий», выполнены	4 P_A следует выбирать только в случае, если выполняются все следующие условия: - оператору предоставляется предупреждение о том, что система защиты вышла из строя; - имеются автономные защищенные зоны (помещения), в которых можно укрыться от опасности, или имеется возможность эвакуации всех в безопасную зону; - время между получением оператором предупреждения и наступлением опасного события превышает 1 час или является абсолютно достаточным для осуществления необходимых действий
Частота запросов (*W*) Число запросов в год (в случае, если бы опасные события происходили в отсутствие Э/Э/ПЭ СБЗС систем)	 W_1 W_2 W_3	Частота запросов: менее 0,1 запросов в год, св. 0,1 *до* 1 запроса в год, св. 1 до 10 запросов в год. Для частоты запросов более 10 запросов в год должна быть более высокая полнота безопасности	5 Цель фактора *W* состоит в оценке частоты опасного события, происходящего без добавления Э/Э/ЭПЭ СБЗС систем. Если частота запросов слишком высока, следует применить другой метод определения УПБ или граф рисков откалибровать. Метод графа рисков — не лучший метод для применения к системам, работающим в режиме с непрерывным запросом. 6 Значение частоты запросов определяют с учетом других рисков, которым подвергаются люди при опасном событии
Примечание — Настоящий пример иллюстрирует применение принципов разработки графов риска. Разработку графов рисков для конкретных применений и конкретных опасностей следует осуществлять с учетом приемлемого риска и сведений, изложенных в разделах К.1—К.6.			

Приложение Л
(справочное)

Определение уровня полноты безопасности. Полуколичественный метод с использованием анализа слоя защиты

Л.1 Общие положения

В настоящем приложении приведена иллюстрация общих принципов метода, называемого анализом слоя защиты (АСЗ), который используют для различных применений.

В одном из применений все соответствующие параметры округляют до более высокого диапазона десятичного порядка (например, вероятность 5×10^{-2} округляют до 10^{-1}). Это очень консервативный подход, который может привести к значительно более высоким значениям УПБ. При неопределенности данных значения всех параметров округляют до следующей большей значащей цифры (например, $5{,}4\times10^{-2}$ округляют до 6×10^{-2}).

АСЗ применяют для определения, достаточны ли требуемые функции безопасности, и если «да», то какой УПБ требуется для каждой функции безопасности. Метод АСЗ адаптируют для удовлетворения применяемых критериев приемлемости риска. При его применении работу начинают со сбора данных по идентификации опасностей и проведения расчетов для каждой идентифицированной опасности путем документирования инициирующих причин и СЗ, предотвращающих или смягчающих опасности. Затем определяют величину общего суммарного риска и необходимость дальнейшего анализа для дополнительного снижения риска. Если дополнительное снижение риска не требуется и если суммарный риск может быть компенсирован Э/Э/ПЭ СБЗС системой, то применение метода АСЗ позволяет определить соответствующий УПБ. Для каждой опасности определяют соответствующий УПБ, обеспечивающий снижение риска до приемлемого уровня. В таблице Л.1 показан типичный формат АСЗ.

Л.2 Воздействующее событие

В колонку 1 таблицы Л.1 вводят описание последствия каждого воздействующего события, определенного из идентификации опасностей.

Л.3 Уровень тяжести последствий

Уровень тяжести последствий опасного события вводят в колонку 2 таблицы Л.1. Уровень тяжести последствий получают из таблицы, которая определяет общее описание уровней тяжести последствий (например, последствия незначительные, тяжелые, катастрофические) с заданным диапазоном последствий и максимальной частотой для каждого уровня тяжести последствий. Фактически эта таблица устанавливает критерии приемлемости для пользователей. Информация будет необходима для определения уровней тяжести последствий и максимальных частот, которые будут определены для событий, влияющих на безопасность и экологические последствия.

Л.4 Инициирующие причины

Все причины, инициирующие воздействующее событие, перечисляют в колонке 3 таблицы Л.1. Воздействующее событие может иметь много инициирующих причин, и все они должны быть перечислены.

Л.5 Вероятность инициирующих причин

Значения вероятности каждой из инициирующих причин, перечисленных в колонке 3 таблицы Л.1, в событиях в год, вводят в колонку 4 таблицы Л.1.

Вероятность инициирующих причин можно вычислить, используя общие данные по частоте (интенсивности) отказов оборудования и зная интервалы между проверками, или используя записи (журналы) по объекту. Низкую вероятность инициирующих причин следует использовать только там, где имеется достаточная статистическая база данных.

Л.6 Слои защиты

Л.6.1 Общие сведения

Каждый СЗ включает в себя комплект оборудования и/или административное управление и функционирует независимо от других слоев.

Особенности проекта, которые снижают вероятность возникновения воздействующего события, происходящего при появлении инициирующих причин, перечисляют сначала в колонке 5 таблицы Л.1.

Для СЗ предусматривают следующие важные характеристики:

- специфичность: СЗ предназначен исключительно для предотвращения или смягчения последствий одного потенциально опасного события, например неконтролируемая реакция, выделение токсичных веществ, потеря защитной оболочки или пожар (к одному и тому же опасному событию может привести несколько причин и, следовательно, действие одного СЗ может инициировать несколько сценариев событий);
- эффективность: СЗ должен быть создан таким, чтобы своими силами он был способен предотвращать нежелательное опасное событие, когда другие меры полностью отказали;

- независимость: СЗ рассматривают независимым от других СЗ, относящихся к другим идентифицированным опасным событиям;

- надежность: СЗ должен быть рассчитан на выполнение тех действий, для которых он был разработан (в проекте рассматривают как случайные, так и систематические виды отказов);

- контролируемость: для СЗ предусматривают регулярную проверку защитных функций (требуются контрольные испытания и техническое обслуживание СЗ).

Л.6.2 Основная система управления

Сведения о системе управления УО устанавливают в колонке 6 таблицы Л.1. Если функция управления предотвращает возникновение воздействующего события при появлении инициирующей причины, то устанавливают среднюю вероятность отказа по запросу PFD_{avg}, на основании которой она разработана. К функции управления не должно быть никакого доверия, если отказ этой функции вызовет запрос к Э/Э/ПЭ СБЗС системе. Следует также отметить, что PFD_{avg}, указанная для функции управления, должна быть ограничена как минимум до 0,1, если функция управления не разработана и функционирует в качестве функции системы безопасности.

Л.6.3 Система тревожной сигнализации

Последний пункт в колонке 6 таблицы Л.1 относится к системе тревожной сигнализации, которая предупреждает оператора и требует его вмешательства. Сигналы тревоги заслуживают доверия только при выполнении следующих условий:

Таблица Л.1 — Типичный формат АСЗ

Последовательность действий	Описание последствия воздействующего события Л.2*	Уровень тяжести последствий Л.3*	Инициирующая причина Л.4*	Вероятность инициирующей причины Л.5*	Слои защиты (СЗ)					Вероятность промежуточного события Л.9*	PFD_{avg}, относящаяся к Э/Э/ЭП СБЗС системы (и УПБ) Л.10*	Приемлемая вероятность смягчения события Л.11*	Примечание
					Общий проект Л.6.1*	Система управления Л.6.2*	Система тревожной сигнализации Л.6.3*	Дополнительное смягчение, ограничение доступа Л.7*	Дополнительное смягчение Л.8*				
1	2	3	4	5	6			7	8	9	10	11	12
1	Превышение скорости ротора приводит к разрушению корпуса	Гибель числа людей, находящихся рядом с корпусом, не превысит двух человек	Полный отказ системы управления скоростью	0,1	1	1	1	0,1	0,1	10^{-3}	5×10^{-3} (УПБ 2 с минимальной PFD_{avg} = $= 5\times10^{-3}$)	10^{-5}	—
			Потеря мощности	1	1	0,1	1	0,1	0,1	10^{-3}			
			Отказ сцепления	0,1	1	0,1	1	0,1	0,1	10^{-4}			
			—	—	—	0,1 недостаточное доверие к системе управления	—	Ограничение заполняемости, для 90 % людей, недостаточно времени	Фатальные последствия возникнут только в случае, если осколки заденут людей	Общая PFD_{avg}= $= 2,1\times10^{-3}$	—	Приемлемая частота летальных исходов не превышает 5×10^{-5}	
2	Повторить экологический анализ риска приведенного выше случая												
3				Предложение — по мере необходимости									
—													
N													

* Обозначения в колонках таблицы соответствуют обозначению раздела или пункта настоящего приложения.

Примечания

1 Степени тяжести последствий могут быть классифицированы как *C* (катастрофические), *E* (обширные), *S* (серьезные) или *M* (незначительные). Вероятность приемлемого смягчения события будет зависеть от степени тяжести последствий.

2 В колонках 5, 9 и 11 приведено вероятное число событий в год.

3 Единицы измерения в колонках 6—8 и 10 — безразмерные. Числа от 0 до 1 — коэффициенты, с помощью которых вероятность события может быть умножена на смягчающее действие соответствующего СЗ, где 1 означает, что смягчающее действие отсутствует, а 0,1 — что коэффициент снижения риска равен 10.

- АС и ПО системы тревожной сигнализации использованы отдельно и независимо от тех, которые используют для системы управления (например, входные платы и процессоры не следует использовать совместно);
- сигнал тревоги отображается с высоким приоритетом в месте постоянного присутствия оператора.

Для признания системы тревожной сигнализации в качестве СЗ принимают во внимание следующее:

- эффективность системы тревожной сигнализации зависит от сложности задачи, которая должна быть выполнена в случае аварийной ситуации, и других задач, которые должны быть выполнены одновременно;
- весовой коэффициент доверия к системе должен быть ограничен для минимальной PFD_{avg}, равный 0,1;
- оператор должен иметь достаточно времени и независимых средств, чтобы успеть купировать опасность (обычно системе тревожной сигнализации не доверяют, если интервал между появлением сигнала тревоги и реализацией опасного события превышает 20 мин).

Л.7 Дополнительное смягчение

Слои смягчения тяжести последствий носят преимущественно механический, конструктивный или процедурный характер. Примеры включают в себя: ограничение доступа; снижение вероятности возгорания; любые другие факторы, которые уменьшают уязвимость лиц, подвергающихся опасности.

Слои смягчения тяжести последствий при их применении могут привести к уменьшению тяжести последствий влияющего события, однако не способны предотвратить возникновение события. Примерами слоев смягчения служат:

- дренчерные установки пожаротушения на случай возникновения пожара;
- система газовой тревоги;
- процедуры эвакуации людей, которые снижают вероятность для людей подвергнуться развивающимся опасным событиям.

При смягчении тяжести последствий следует принимать во внимание так называемый коэффициент присутствия человека в зоне, наиболее подверженной опасности. Этот коэффициент получают путем определения количества часов пребывания человека в опасной зоне в год и деления на 8760 ч в год.

Соответствующие PFD_{avg} или их эквиваленты должны быть определены для всех слоев смягчения последствий опасных событий и приведены в колонках 7 и 8 таблицы Л.1.

Л.8 Промежуточная вероятность события

Промежуточную вероятность события по каждой причине рассчитывают путем умножения на коэффициенты по частоте в год и результаты включают в колонку 9 таблицы Л.1 в соответствии с факторами:

- уязвимость лица, подверженного наибольшему опасному воздействию;
- вероятность инициирования воздействия (колонка 5);
- PFD_{avg} СЗ и слоев смягчения последствий опасных событий (колонки 6, 7 и 8 в таблице Л.1).

Общую промежуточную частоту событий рассчитывают путем добавления промежуточных частот событий для каждой причины.

Общую промежуточную частоту событий сравнивают с приемлемой частотой риска для соответствующего уровня тяжести последствий. Если общая промежуточная частота превышает приемлемую частоту, то потребуется снижение риска. В этом случае до применения слоев безопасности в виде Э/Э/ПЭ СБЗС систем следует рассмотреть более безопасные методы и ситуации.

Если промежуточные средние вероятности опасных событий не могут быть уменьшены ниже максимальных критериев частоты, то потребуется применение Э/Э/ПЭ СБЗС системы.

Л.9 Требуемый уровень полноты безопасности

Если применение Э/Э/ПЭ СБЗС системы необходимо, требуемый УПБ может быть определен следующим образом:

- вначале максимальную частоту для связанного с безопасностью уровня тяжести последствий разделяют на общую промежуточную вероятность событий для определения требуемой PFD_{avg};
- затем численное целевое значение PFD_{avg} может быть использовано в спецификации требований безопасности вместе с соответствующим связанным УПБ. Такой связанный УПБ может быть использован из таблиц 1 и 2 ГОСТ 34332.2;
- если численное значение PFD_{avg} не должно быть в спецификации требований к технологическому процессу и потребуется указать только УПБ, то УПБ необходимо будет поднять выше на один уровень относительно указанной УПБ таким образом, чтобы при всех значениях УПБ было достигнуто адекватное снижение риска;
- если для достижения приемлемого риска требуется PFD_{avg}, большая или равная 0,1, то функция относится к классификации «Специальные требования к полноте безопасности отсутствуют».

Л.10 Приемлемая вероятность смягчения события

Приемлемая вероятность смягчения события зависит от степени тяжести последствий. Она зависит от принятых критериев приемлемого риска [см. критерии приемлемого риска в разделе Д.2 (приложение Д)].

Приложение М
(справочное)

Определение уровня полноты безопасности. Качественный метод — матрица тяжести последствий опасных событий

М.1 Общие положения

Численный метод, описанный в приложении И, не применяют, когда риск или его частотная часть не могут быть определены количественно. В настоящем приложении описан метод матрицы серьезности (тяжести последствий) опасного события, которая представляет собой качественный метод, позволяющий определить УПБ Э/Э/ПЭ СБЗС системы, исходя из знаний факторов риска, связанного с УО и с системой управления УО. Метод применим, в частности, когда модель риска соответствует модели, показанной на рисунках Д.1 и Д.2 (приложение Д).

В методе, изложенном в настоящем приложении, предполагается, что каждая Э/Э/ПЭ СБЗС система и прочее средство уменьшения риска не зависимы друг от друга.

Настоящее приложение предназначено для иллюстрации общих принципов и описания того, как такая матрица может быть разработана с использованием детальных знаний о конкретных параметрах, имеющих отношение к конструкции систем и средств.

М.2 Матрица степени тяжести последствий опасных событий

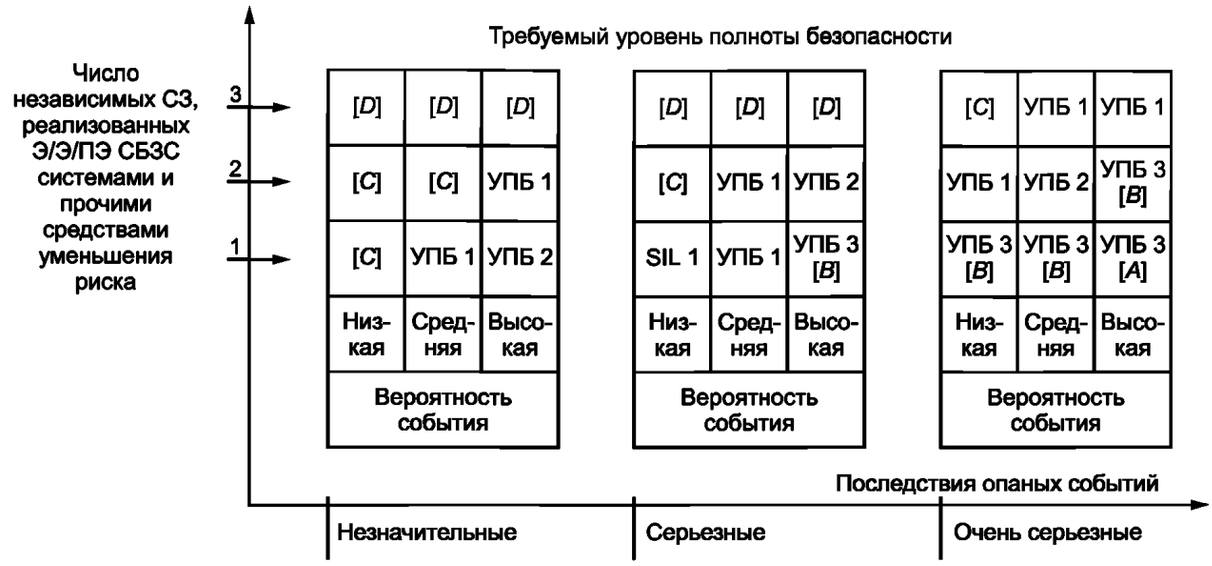
В основу метода матрицы степени тяжести последствий опасных событий положены следующие обязательные для выполнения условия:

- Э/Э/ПЭ СБЗС системы и прочие средства уменьшения риска являются независимыми;
- каждая из СБЗС систем, основанных на Э/Э/ПЭ технологиях и неэлектрических технологиях, а также каждое прочее средство уменьшения риска рассматривается в качестве отдельного СЗ, который обеспечивает соответствующее частичное снижение риска, как показано на рисунке Д.1 (приложение Д).

Примечание — Данное условие считают выполненным только в случае, если обеспечено регулярное проведение контрольных испытаний каждого СЗ;

- при добавлении одного СЗ (см. второе перечисление) достигается улучшение величины полноты безопасности на один десятичный порядок;
- используется только одна Э/Э/ПЭ СБЗС система (но, возможно, в сочетании с прочим средством уменьшения риска), для которой данный метод устанавливает необходимый УПБ.

Матрица степени тяжести последствий опасных событий, построенная при выполнении перечисленных условий, представлена на рисунке М.1. Она заполнена данными, иллюстрирующими общие принципы. В случае применения данного метода для каждой конкретной ситуации должна быть построена аналогичная матрица, разработанная и откалиброванная в приемлемых критериях риска, применимых к данной конкретной ситуации.



[*A*] — одна СБЗС система с УПБ 3 функции безопасности не обеспечивает достаточного снижения риска на этом уровне риска, для снижения риска необходимы дополнительные меры (см. [*D*]); [*B*] — одна СБЗС система с УПБ 3 функции безопасности может не обеспечивать достаточного снижения риска на этом уровне риска, для снижения риска необходимы дополнительные меры (см. [*D*]); [C] — независимый уровень защиты SIS, вероятно, не требуется; [*D*] — данный подход не пригоден для УПБ 4

Рисунок М.1 — Матрица степени тяжести последствий опасных событий (иллюстрация принципа)

Библиография

[1] Технический регламент Таможенного союза ТР ТС 002/2011 — О безопасности высокоскоростного железнодорожного транспорта

[2] Технический регламент Таможенного союза ТР ТС 003/2011 — О безопасности инфраструктуры железнодорожного транспорта

[3] Технический регламент Таможенного союза ТР ТС 014/2011 — Безопасность автомобильных дорог

[4] Технический регламент Евразийского экономического союза «О безопасности зданий и сооружений, строительных материалов и изделий» (проект)

[5] Руководство ИСО/МЭК 51:2014 — Аспекты безопасности. Руководящие указания по включению их в стандарты. (ISO/IEC Guide 51:2014 Safety aspects: Guidelines for their inclusion in standards)

gost.e-ecolog.ru _catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53940 (доступ 24.09.2016).

УДК 621.5:814.8:006.354

МКС 13.100,
13.110,
13.200,
13.220,
13.310,
13.320,
91.120.99

NEQ

Ключевые слова: системы, связанные с безопасностью зданий и сооружений; функциональная безопасность систем, связанных с безопасностью зданий и сооружений; полнота безопасности; уровни полноты безопасности; основные положения

БЗ 8—2017/41

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 26.10.2018. Подписано в печать 12.11.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,45.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru