ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53195.1— 2008

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 1

Основные положения

Издание официальное

БЗ 8—2008/206

Москва
Стандартинформ
2009

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 РАЗРАБОТАН Всемирной Академией Наук Комплексной Безопасности и ООО НТЦ «Стройинновация».

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 439 «Средства автоматизации и системы управления» при поддержке Технического комитета по стандартизации ТК 465 «Строительство»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 653-ст.

4 В настоящем стандарте использованы основные нормативные положения следующих международных стандартов:

- МЭК 61508-4:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины, определения, сокращения» (IEC 61508-4:1998 Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 4: Definitions and abbreviations);
- МЭК 61508-5:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности» (IEC 61508-5:1998 Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels);
- Руководство ИСО/МЭК 51:1999 Аспекты безопасности. Руководящие указания по включению их в стандарты (ISO/IEC Guide 51:1999 «Safety aspects — Guidelines for their inclusion in standards)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

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 5
5 Взаимосвязь систем 5
5.1 Общие положения 5
5.2 Составляющие зданий и сооружений 5
5.3 Жизненные циклы СБЗС-систем 6
6 Проектные опасности 7
7 Риск и полнота безопасности 7
7.1 Риск 7
7.2 Порядок достижения приемлемого риска 8
8 Принцип установления приемлемого риска 10
9 Определение уровней полноты безопасности 10
Приложение А (справочное) Системы 11
Приложение Б (справочное) Источники, виды и характер опасностей 13
Приложение В (справочное) Факторы риска 14
Приложение Г (справочное) Критерий и категории тяжести последствий 16
Приложение Д (справочное) Принцип разумной достаточности и приемлемого риска 17
Приложение Е (справочное) Определение уровней полноты безопасности: количественный метод 20
Приложение Ж (справочное) Определение уровней полноты безопасности: качественный метод . . 24
Приложение И (справочное) Определение уровней полноты безопасности — качественный метод: матрица критичности опасных событий 28

Введение

Современные здания и сооружения — объекты строительного производства — представляют собой сложные системы, включающие в себя систему конструкций и ряд систем в разных сочетаниях, в том числе инженерные системы жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, безопасности и другие системы. Эти системы взаимодействуют друг с другом, с внешней и внутренней средами.

В отличие от продукции промышленного производства объекты строительного производства 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 и средств для снижения риска причинения вреда до уровня приемлемого риска и поддержанием этого уровня в течение периода эксплуатации или использования этих объектов. К техническим средствам снижения риска относятся системы, связанные с безопасностью зданий и сооружений, состоящие из электрических и/или электронных компонентов, которые в течение многих лет используются для выполнения функций безопасности. Кроме них и вместе с ними используются системы, основанные на других (гидравлических, пневматических) технологиях, а также внешние средства уменьшения риска. Для решения задач безопасности зданий и сооружений во все бóльших объемах используются программируемые электронные, т. е. компьютерные системы.

Настоящий стандарт распространяется на системы, связанные с безопасностью зданий и сооружений, и устанавливает основные положения по определению требований к функциональной безопасности этих систем.

Настоящий стандарт:

- рассматривает здание и сооружение как сложную систему, определяет состав, роль и место систем, связанных с безопасностью зданий и сооружений, в достижении безопасности объекта;
- устанавливает общий подход к вопросам обеспечения безопасности зданий и сооружений, основанный на снижении риска с применением связанных с безопасностью систем и внешних средств уменьшения риска;
- содержит перечень опасностей и угроз, критерии и категории тяжести последствий при реализации опасных событий;
- включает концепцию установления допустимого риска на основе принципа разумной достаточности;
- содержит описание основных принципов оценки риска и оценки полноты безопасности.

Настоящий стандарт рассчитан на любой диапазон сложности систем, связанных с безопасностью зданий и сооружений, и ориентирован на комплексное обеспечение безопасности объектов.

Настоящий стандарт является первым стандартом, входящим в комплекс из семи стандартов с общим наименованием «Безопасность функциональная связанных с безопасностью зданий и сооружений систем» (Часть 1 — Основные положения). Другие стандарты этого комплекса следующие:

Часть 2 — Общие требования;

Часть 3 — Требования к системам;

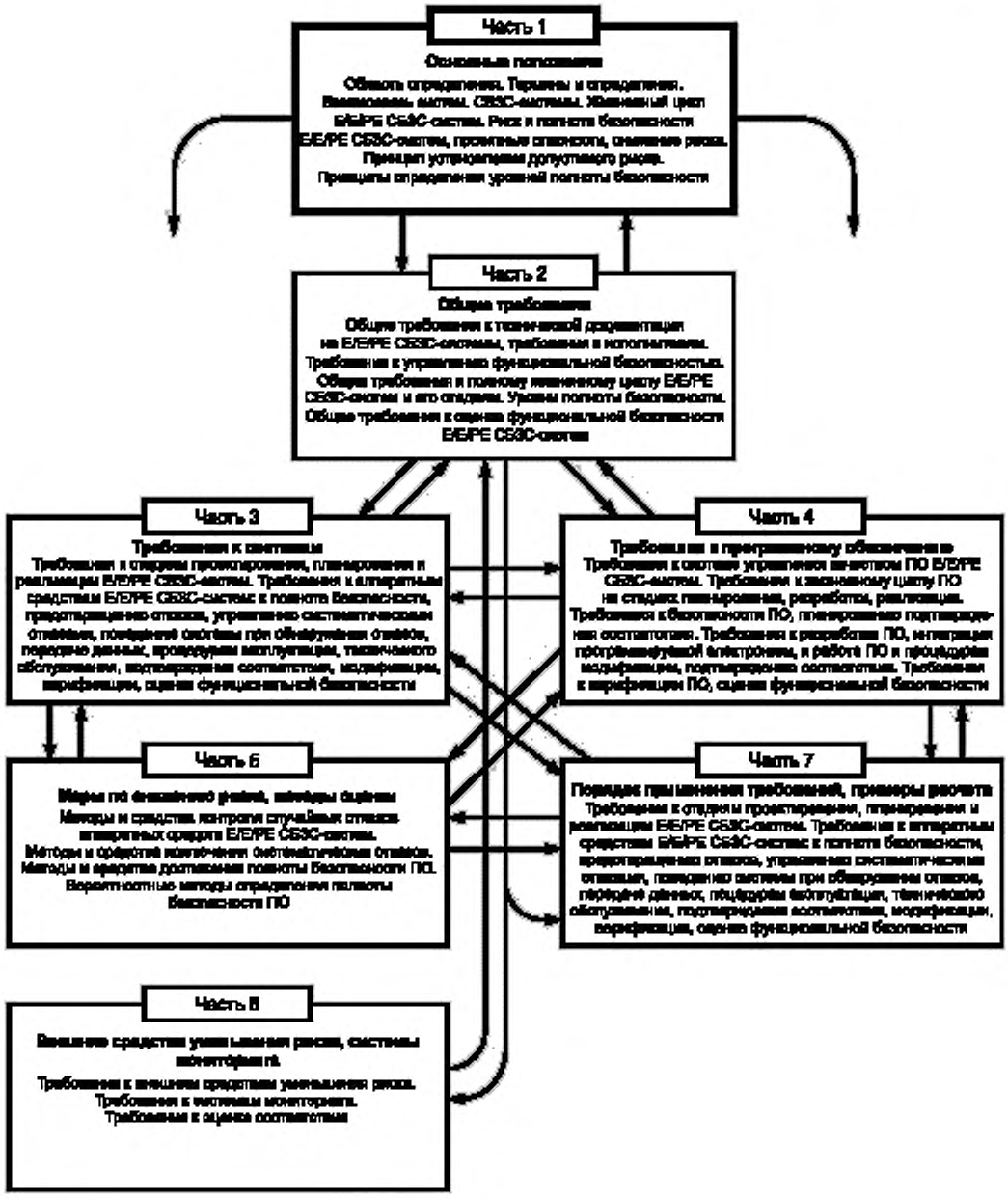
Часть 4 — Требования к программному обеспечению;

Часть 5 — Меры по снижению риска, методы оценки;

Часть 6 — Внешние средства уменьшения риска и системы мониторинга;

Часть 7 — Порядок применения требований к системам и примеры расчетов.

Общая структура комплекса стандартов приведена ниже.


Часть 1
Основные положения
Область определения. Термины и определения.
Взаимосвязь систем. СЕЗС-системы. Жизненный цикл
Е/Э/ПрЭ СЕЗС-систем. Риск и полнота безопасности
Е/Э/ПрЭ СЕЗС-систем, приемлемые опасности, снижение риска.
Принцип установления допустимого риска.
Принципы определения уровней полноты безопасности
Часть 2
Общие требования
Общие требования к технической документации
на Е/Э/ПрЭ СЕЗС-системы, требования к испытаниям.
Требования к управлению функциональной безопасностью.
Общие требования к полному жизненному циклу Е/Э/ПрЭ
СЕЗС-систем и его стадиям. Уровни полноты безопасности.
Общие требования к оценке функциональной безопасности
Е/Э/ПрЭ СЕЗС-систем
Часть 3
Требования к системам
Требования к стадиям проектирования, планирования и
реализации Е/Э/ПрЭ СЕЗС-системы. Требования к аппаратным
средствам Е/Э/ПрЭ СЕЗС-систем к полноте безопасности,
предотвращению отказов, управлению систематическими
отказами, поведению системы при обнаружении отказов,
передаче данных, процедурам эксплуатации, технического
обслуживания, подтверждения соответствия, модификации,
верификации, оценке функциональной безопасности
Часть 4
Требования к программному обеспечению
Требования к системе управления качеством ПО Е/Э/ПрЭ
СЕЗС-систем. Требования к жизненному циклу ПО
на стадиях планирования, разработки, реализации.
Требования к безопасности ПО, планированию подтверждения
соответствия. Требования к разработке ПО, интеграции
программируемой электроники, и работе ПО и процедурам
модификации, подтверждению соответствия. Требования
к верификации ПО, оценке функциональной безопасности
Часть 6
Меры по снижению рисков, методы оценки
Методы и средства контроля случайных отказов
аппаратных средств Е/Э/ПрЭ СЕЗС-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 расчета
Требования к стадиям проектирования, планирования и
реализации Е/Э/ПрЭ СЕЗС-систем. Требования к аппаратным
средствам Е/Э/ПрЭ СЕЗС-систем к полноте безопасности,
предотвращению отказов, управлению систематическими
отказами, поведению системы при обнаружении отказов,
передаче данных, процедурам эксплуатации, технического
обслуживания, подтверждения соответствия, модификации,
верификации, оценке функциональной безопасности
Часть 5
Внешние средства уменьшения риска, системы
мониторинга
Требования к внешним средствам уменьшения риска.
Требования к системам мониторинга.
Требования к оценке соответствия

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 1

Основные положения

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

Дата введения — 2010—01—01

1 Область применения

Настоящий стандарт распространяется на электрические, электронные, программируемые электронные системы, связанные с безопасностью зданий и сооружений (далее E/E/PE СБЗС-системы), устанавливаемые или установленные во вновь возводимых или реконструируемых зданиях и сооружениях (объектах).

Настоящий стандарт устанавливает основные положения по определению требований к функциональной безопасности связанных с безопасностью зданий и сооружений систем (далее СБЗС-систем).

Настоящий стандарт распространяется на E/E/PE 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 SIL1 — самым низким уровнем полноты безопасности по ГОСТ Р 53195.2.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 53195.2—2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Общие требования

ГОСТ Р ИСО 9000—2008 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001—2008 Системы менеджмента качества. Требования

ГОСТ Р ИСО 9004—2001 Системы менеджмента качества. Рекомендации по улучшению деятельности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. 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.

Издание официальное

3 Термины и определения

В настоящем стандарте использованы термины с соответствующими определениями, применяемые в комплексе стандартов «Безопасность функциональная связанных с безопасностью зданий и сооружений систем».

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

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

3.3 **внешнее средство уменьшения риска;** ВСУР: (external risk reduction facility): Средство, предназначенное для снижения риска, которое является отдельным и отличным от электрической, электронной, программируемой электронной связанной с безопасностью системы (например, противопожарная преграда, ограда, ров).

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

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

3.6 **жизненный цикл связанной с безопасностью зданий и сооружений системы;** жизненный цикл СБЗС-системы (safety lifecycle): Последовательность следующих друг за другом необходимых процессов создания и использования связанной с безопасностью системы, проходящих в течение интервала времени, который начинается со стадии разработки концепции проекта системы или средства и заканчивается, когда эта система или средство выведены из эксплуатации.

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

3.8 **инженерная система (здания или сооружения):** Одна из систем здания или сооружения, предназначенная для жизнеобеспечения (например, система водоснабжения, система канализации, система теплоснабжения, система электроснабжения, система электроосвещения, система вентиляции и др.), выполнения процессов (система технологического оборудования — на объектах производственного назначения), поддержания комфорта (система кондиционирования воздуха, система вертикального транспорта, система тепловоздушных завес и т.п.), энерго- и ресурсосбережения (система учета потребления энергоресурсов, система учета водопотребления, система тепловых насосов, система управления светом и др.) обеспечения безопасности (система пожарной сигнализации, охранной сигнализации, система пожаротушения, дымоудаления, тревожного оповещения, контроля и управления доступом и др.).

Примечания

1 Более сложные инженерные системы могут включать в себя менее сложные инженерные системы, которые являются их подсистемами.

2 Человек (оператор) может рассматриваться как часть системы или подсистемы.

3.9 **использование по назначению:** 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.

3.10 **комплексная безопасность:** Безопасность при наличии нескольких видов и/или источников опасности.

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

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

3.13 **мера безопасности** (safety measure): Мера, применяемая для снижения риска, приводящая к уменьшению риска за счет выполнения норм и правил и/или выбора эффективных проектных решений.

и/или применения связанных с безопасностью систем, внешних 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.

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

3.15 **нарушитель** (intruder): Лицо, осуществляющее попытку вторжения или несанкционированного действия либо осуществившее такие действия.

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

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

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

3.19 **общая оценка риска** (total risk assessment): Полный процесс анализа риска и оценки риска.

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

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

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

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

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

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

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

3.27 **полнота безопасности (системы)** (safety integrity): Вероятность удовлетворительного выполнения связанной с безопасностью системой функции или функций безопасности в конкретных условиях и в пределах конкретного интервала времени.

3.28 **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.

3.29 **полнота безопасности программного обеспечения;** полнота безопасности ПО (software safety integrity): Составляющая полноты безопасности связанной с безопасностью системы по отношению к отказам программного обеспечения, проявляющимся в опасном режиме при заданных условиях и в пределах заданного интервала времени.

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

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

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

3.33 **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.

3.34 **проектная опасность:** Опасность, предусмотренная при проектировании и учитываемая при оценке риска на этапах жизненного цикла системы, при оценке и подтверждении соответствия требованиям безопасности.

3.35 **программируемая электроника** (programmable electronics; PE): Электронное средство, основанное на использовании компьютерной технологии, и которое может включать в себя аппаратные средства и программное обеспечение, а также устройства ввода и/или вывода.

3.36 **риск управляемого оборудования;** риск УО (equipment under control risk; EUC risk): Риск, связанный с управляемым оборудованием или с взаимодействием связанной с безопасностью системы с системой управления управляемым оборудованием.

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

Примечания

1 Подсистема в настоящем термине и термине 3.38 также является системой, которая входит составной частью в более крупную систему; подсистема, в свою очередь, может состоять из ряда менее крупных подсистем, которые также могут быть системами. Например, система охраны периметров может включать в свой состав подсистему охраны внешнего периметра объекта и подсистемы охраны периметров отдельных зон, а каждая из этих подсистем может содержать кабельные вибрационные и/или радиоволновые подсистемы охраны периметров и подсистему телевизионного наблюдения, которая, в свою очередь, может включать в свой состав подсистему охранного освещения. При этом каждая из рассмотренных подсистем является связанной с безопасностью системой, реализующей определенную функцию или функции безопасности.

2 Человек (оператор, пользователь) может входить в состав системы или подсистемы как ее часть.

3.38 **связанная с безопасностью зданий и сооружений система [подсистема];** СБЗС-система [подсистема]: Связанная с безопасностью система [подсистема], установленная в зданиях и сооружениях, взаимодействующая с системами или подсистемами этих объектов, с их составляющими и средой.

3.39 **система управления управляемым оборудованием;** система управления УО (equipment under 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.

3.40 **техногенная опасность:** Опасность, обусловленная объектами, созданными людьми и процессами их деятельности.

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

Примечание — Уровень полноты безопасности SIL 4 характеризует наибольшую полноту безопасности, SIL 1 — наименьшую полноту безопасности.

3.42 **функциональная безопасность** (functional safety): Часть безопасности, относящаяся к управляемому оборудованию и системе управления управляемым оборудованием связанной с безопасностью здания или сооружения системы при выполнении функции безопасности.

3.43 **функция безопасности** (safety function): Функция, выполняемая связанной с безопасностью системой для достижения или поддержания безопасного состояния управляемого оборудования при определенном опасном событии.

Примечания

1 Функция безопасности характеризуется назначением (что выполняет функция) и полнотой безопасности — вероятностью удовлетворительного выполнения этой назначенной функции.

2 Функциональная безопасность связанной с безопасностью здания и сооружения системы обеспечивается при удовлетворительном выполнении назначенной функции безопасности.

3 Функция безопасности связанной с безопасностью системы завершается действием управляемого оборудования, приводящим к снижению риска причинения вреда и/или тяжести последствий.

3.44 **электрическая [электронная, программируемая электронная] система;** E/E/PE-система (electrical/electronic/programmable electronic system; E/E/PES): Система, предназначенная для управления, защиты или мониторинга, содержащая одно или несколько электрических и/или электронных, и/или программируемых электронных устройств, включающая все элементы системы, такие как источники пита-

ния, сенсоры, входные устройства, устройства ввода, коммуникационные магистрали, устройства вывода, устройства привода, выходные или оконечные устройства.

3.45 **электрический [электронный, программируемый электронный];** E/E/PE (electrical/electronic/programmable electronic; E/E/PE) — основанный на электрической и/или электронной, и/или программируемой электронной технологии.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и обозначения:

КР — крайне рекомендованный (в отношении уровня независимости);
НР — не рекомендованный (в отношении уровня независимости);
КСБ — комплексная система безопасности;
ПО — программное обеспечение;
СБС — связанная с безопасностью система;
СБЗС-система — связанная с безопасностью здания и сооружения система;
УО — управляемое оборудование.

международные обозначения:

ALARP — низкий настолько, насколько это практически рационально (в отношении уровня риска);
E/E/PE — электрическая и/или электронная, и/или программируемая электронная;
E/E/PES — электрическая и/или электронная, и/или программируемая электронная система;
EUC — управляемое оборудование;
HR — крайне рекомендованный (в отношении уровня независимости);
NR — не рекомендованный (в отношении уровня независимости);
PES — программируемая электронная система;
SIL — уровень полноты безопасности.

5 Взаимосвязь систем

5.1 Общие положения

5.1.1 Здание и сооружение в рамках настоящего стандарта рассматриваются как сложная система, включающая в себя систему строительных конструкций, инженерные системы жизнеобеспечения, реализации процессов, энерго- и ресурсосбережения, обеспечения безопасности. Системы, входящие в состав здания и сооружения, взаимодействуют между собой, с внешней и внутренней средами. Здание и сооружение взаимодействуют с внешним окружением и средой на градостроительном, ресурсном, структурном, функциональном, информационном уровнях с учетом географических, геологических, климатических и иных местных условий.

СБЗС-системы, входящие в состав зданий и сооружений, выполняют функции безопасности и снижают риск причинения вреда жизни и здоровью людей (животных, растений), имуществу, окружающей среде.

5.2 Составляющие зданий и сооружений

5.2.1 Система конструкций зданий и сооружений

Система конструкций зданий и сооружений должна обеспечивать выполнение назначенных функций и соответствовать требованиям, определенным в утвержденных в установленном порядке техническом задании, технических условиях и проектной документации на архитектурно-строительные (АС), архитектурные (АР) решения.

5.2.2 Инженерные системы

5.2.2.1 В состав инженерных систем жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, поддержания комфорта входят системы, приведенные в разделе А.1 приложения А.

5.2.2.2 Системы жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, поддержания комфорта должны обеспечивать выполнение назначенных функций, определенных в утвержденных в установленном порядке техническом задании, технических условиях и проектной документации на объект.

5.2.2.3 Каждая из инженерных систем и/или подсистем может содержать собственные средства и системы защиты, предохраняющие эксплуатирующий персонал и пользователей здания и 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 В состав инженерных систем обеспечения безопасности зданий и сооружений входят E/E/PE СБЗС-системы и подсистемы, приведенные в разделе А.2 приложения А.

5.2.3.2 СБЗС-системы и подсистемы совместно с внешними средствами уменьшения риска должны обеспечивать снижение остаточного риска, обусловленного природными, техногенными и антропогенными опасностями, возникающими из-за внешних и внутренних воздействий на систему конструкций и другие инженерные системы, до уровня приемлемого риска, установленного в утвержденных в установленном порядке технических условиях (специальных технических условиях), и/или задании на проектирование объекта (рисунок 1).

Примечание — Уровень приемлемого риска, устанавливаемый в технических условиях (специальных технических условиях и/или в задании на проектирование объекта не должен превышать уровень максимально допустимого риска, установленного в технических регламентах.

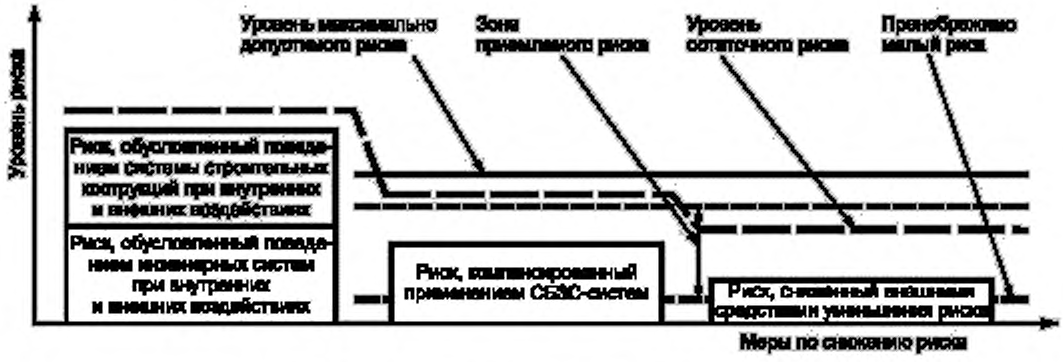


Рисунок 1 — Снижение риска до уровня приемлемого риска

5.2.3.3 Взаимодействующие программируемые электронные СБЗС-системы и подсистемы должны обладать информационной совместимостью и поддерживать единые унифицированные протоколы обмена информацией.

5.2.3.4 Все СБЗС-системы должны надежно выполнять все предусмотренные для них функции безопасности в условиях взаимодействия этих систем и подсистем (смежных с ними систем и подсистем), при взаимовлиянии их друг на друга, в том числе с учетом электромагнитной совместимости, обеспечивая заданный уровень полноты безопасности.

5.2.3.5 Состав СБЗС-систем, применяемых в отдельных зданиях и сооружениях в зависимости от категорий риска объектов и вероятной тяжести последствий при реализации опасных событий, должен определяться на стадии проектирования с учетом свойств систем и требований, установленных отдельными стандартами на эти системы.

5.3 Жизненные циклы СБЗС-систем

5.3.1 Жизненный цикл каждой СБЗС-системы и подсистемы включает стадии:

- разработки концепции;
- анализа опасностей и оценки рисков;
- проектирования;
- реализации системы или подсистемы;
- установки (монтажа) оборудования;
- интеграции и пуско-наладки систем;
- оценки и подтверждения соответствия;
- ввода в эксплуатацию;
- эксплуатации;
- технического обслуживания;
- реконструкции (видоизменения, модификации);

- вывода из эксплуатации;
- утилизации.

За один жизненный цикл системы конструкций здания и сооружения может проходить несколько жизненных циклов СБЗС-систем.

5.3.2 Общие требования к отдельным стадиям жизненного цикла СБЗС-систем должны соответствовать требованиям, установленным в стандарте на общие требования к функциональной безопасности этих систем.

5.3.3 Требования к СБЗС-системам на стадиях разработки и реализации проекта, мерам по снижению рисков, методам оценки полноты безопасности и подтверждения соответствия должны соответствовать требованиям, установленным в стандарте на требования к системам.

5.3.4 Требования к программному обеспечению СБЗС-систем на стадии его разработки и реализации, методы достижения полноты безопасности и оценки соответствия должны удовлетворять требованиям, установленным в стандарте на требования к программному обеспечению этих систем.

5.3.5 Требования к внешним средствам уменьшения риска и системам мониторинга конструкций и оборудования должны удовлетворять требованиям, установленным в стандарте на системы мониторинга конструкций и внешние средства уменьшения риска.

5.3.6 На стадии эксплуатации, в периодах технического обслуживания СБЗС-систем, их видоизменения, модификации, ремонта или реконструкции, в периодах ремонта объекта, должны быть предусмотрены дополнительные меры по поддержанию функциональной безопасности систем и объекта на приемлемом уровне.

6 Проектные опасности

6.1 Для каждого здания и сооружения на стадии разработки технических условий (специальных технических условий) и/или задания на проектирование должны быть установлены виды проектных опасностей, модели нарушителя и модели угроз антропогенного характера с учетом местных условий.

6.2 Проектные опасности для СБЗС-систем конкретного здания или сооружения, должны быть установлены проектировщиком в соответствии с требованиями технического задания и технических условий (специальных технических условий) на объект.

6.3 При установлении проектных опасностей и выборе СБЗС-систем должны быть учтены: назначение, функции, конструкция, сложность объекта, его состав (см. приложение А), расположение на местности, местные условия, виды и характер опасностей (см. приложение Б), факторы риска (см. приложение В) и возможная тяжесть последствий при реализации опасных событий (см. приложение Г).

6.4 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, в том числе с учетом моделей нарушителя и моделей угроз.

7 Риск и полнота безопасности

7.1 Риск

7.1.1 Риск, связанный с реализацией опасного события, должен определяться как функционал f, характеризующийся частотой или вероятностью реализации опасного события и последствиями этого события (тяжестью причиненного вреда) на основе выражения:

$$R_i = f(F_i, C_i), \quad (1)$$

где R_i — риск, возникающий в результате реализации i-го опасного события,

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

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

f — функционал.

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

7.1.3 Комплексное обеспечение безопасности зданий и сооружений при совокупности опасных событий должно достигаться за счет снижения суммарного риска до уровня приемлемого риска.

7.1.4 Установление максимально допустимого риска может быть осуществлено на основе концепции разумной достаточности (ALARP) (см. приложение Д).

7.1.5 Значение максимально допустимого риска, связанного с эксплуатацией или использованием зданий и сооружений, пребыванием людей, нахождением имущества, животных и растений на этих объектах и прилегающих территориях, устанавливается техническим регламентом о безопасности зданий и сооружений.

7.1.6 Значения приемлемого риска для СБЗС-систем должны определяться на стадии проектирования с учетом требований раздела 6.

7.2 Порядок достижения приемлемого риска

7.2.1 Приемлемый риск должен достигаться с помощью итеративного процесса общей оценки риска и снижения риска в соответствии с концепцией безопасности, установленной Руководством ИСО/МЭК 51 (рисунок 2) [3]. Этот процесс должен продолжаться до тех пор, пока риск не будет снижен до уровня приемлемого риска.

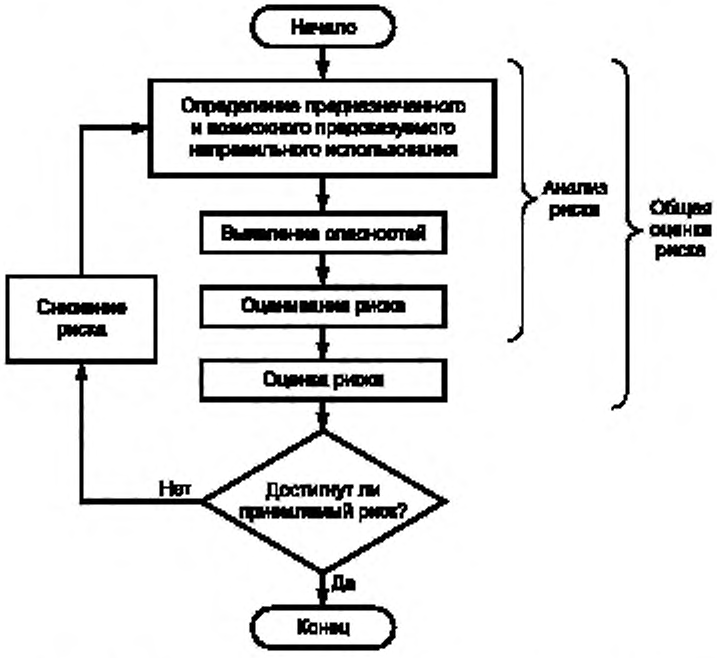


Рисунок 2 — Итеративный процесс общей оценки и снижения риска

7.2.2 Для сокращения риска до уровня приемлемого риска следует осуществить следующую последовательность действий:

а) определить возможную группу или группы пользователей зданиями и сооружениями (включая рабочих, служащих; для жилых, общественных и многофункциональных зданий и сооружений — жильцов, посетителей, временно пребывающих лиц, в том числе группы людей с ограниченными возможностями, группу пожилых людей и детей);

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

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

г) определить проектные опасности с учетом моделей опасностей и моделей нарушителей;

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

е) 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;

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

и) 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);

к) принять меры по снижению риска до уровня приемлемого риска, если риск окажется выше максимально допустимого риска.

7.2.3 При выборе мер по снижению риска на стадии разработки проекта (рисунок 3) следует руководствоваться следующими приоритетами:

1) разработка проекта с эффективными решениями по безопасности;

2) применение защитных устройств, средств или систем;

3) предоставление информации пользователям, эксплуатирующему персоналу и лицам, осуществляющим техническое обслуживание систем.



Рисунок 3 — Меры по снижению риска

Примечание — При проектировании СБЗС-систем в качестве начального риска (см. рисунок 3), может быть принят остаточный риск, оставшийся в результате предварительно принятых конструктивных и объемно-планировочных решений зданий и сооружений, утвержденных в установленном порядке.

7.2.4 На стадии проектирования расчет на возможное применение дополнительных защитных устройств, средств, систем, индивидуальных средств защиты и предоставление информации пользователям, эксплуатирующему персоналу и персоналу, осуществляющему техническое обслуживание 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, должны осуществляться в соответствии с системами менеджмента качества, принятыми на предприятиях — исполнителях, не противоречащими требованиям ГОСТ Р ИСО 9000, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 9004.

7.2.5 Для снижения риска на стадиях реализации проекта и эксплуатации могут быть приняты следующие меры:

1) применение дополнительных защитных СБЗС-систем и средств;

2) обучение персонала, лиц, осуществляющих техническое обслуживание, и пользователей;

3) применение индивидуальных средств защиты;

4) организация безопасной эксплуатации объекта и безопасного пользования им (см. рисунок 3).

Примечание — На этих стадиях 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 Принцип установления приемлемого риска

8.1 Уровень приемлемого риска, связанного с использованием и эксплуатацией здания и сооружения, должен соответствовать требованиям соответствующего технического регламента, требованиям 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 (см. приложение Д).

9 Определение уровней полноты безопасности

9.1 Уровни полноты безопасности СБЗС-систем должны быть определены на стадии проектирования.

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

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

9.4 Для инженерных расчетов полноты безопасности СБЗС-систем следует применять стандартизованные или общепризнанные методы.

Приложение А
(справочное)

Системы

А.1 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 система (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 учреждений);
- видеоконференц-система (в административных, общественных, многофункциональных зданиях, зданиях учебных заведений и научных учреждений);
- видеопроекции (в административных, общественных, многофункциональных зданиях, зданиях учебных заведений и научных учреждений);
- кинофикации (в кинотеатрах, зрелищных зданиях и сооружениях);
- перевода речи (в зданиях учебных и научных заведений);
- звуковая студия (в зданиях учебных заведений, научных учреждений, сооружениях телерадиовещания);
- телевизионная студия (в зданиях учебных заведений, научных учреждений, сооружениях телерадиовещания);
- видеостудия (в зданиях учебных и научных учреждений, телерадиовещания);
- пневмопочта;
- локальных вычислительных сетей;
- узел подключения внешних интегральных сетей (в жилых, административных и общественных зданиях, зданиях учебных заведений и научных учреждений);

- управления товарооборотом (в торговых заведениях);
- управления гостиницей (в гостиницах);
- структурированная кабельная сеть;
- электрочасификации;
- реализации производственных, технологических и иных процессов;
- интеграции подсистем.

А.2 Системы обеспечения безопасности

В состав систем обеспечения безопасности зданий и сооружений входят следующие СБЗС-системы или подсистемы:

- аварийного освещения;
- автоматизации противопожарного водоснабжения;
- автоматического водяного пожаротушения;
- пожарной сигнализации;
- автоматизации противодымной защиты;
- контроля тока утечки;
- контроля воздушно-газовой среды, в том числе:
    - контроля окиси углерода (CO),
    - ядовитых паров и газов,
    - взрывоопасных газов и паров,
    - агрессивных паров и газов,
    - 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 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;
- структурированная кабельная сеть;
- защиты информации;
- интегрирования систем безопасности[1)];
- комплексная система безопасности.

[1)] При объединении двух или более систем или подсистем.

Приложение Б
(справочное)

Источники, виды и характер опасностей

При рассмотрении связанных с безопасностью зданий и сооружений систем в зависимости от местных условий следует учитывать:

1) 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.

2) Техногенные опасности:

- механическую опасность, например, нарушения прочности и устойчивости конструкций;
- опасность пожара;
- опасность взрыва — при наличии или образовании взрывоопасных веществ и материалов;
- промышленную опасность — для потенциально опасных производств, процессов и технологий;
- термическую опасность — для объектов, где имеются высокотемпературные источники;
- химическую опасность — для химических производств, складов, хранилищ, объектов с большими массами химически активных веществ;
- электрическую опасность — для всех объектов, где используется электричество;
- опасность излучений — при наличии источников излучений;
- биологическую опасность — при наличии источников биологической опасности;
- ядерную опасность — для ядерных объектов, объектов производства, переработки и хранения ядерных материалов;
- радиационную опасность — для объектов, на территории которых имеются радиоактивные вещества и материалы.

3) Антропогенные опасности:

- вызванные прогнозируемым неправильным использованием систем и их составляющих:
  - эксплуатирующим, обслуживающим персоналом различных групп,
  - пользователями различных групп и контактными группами;
  - вызванные злонамеренными действиями:
  - криминального характера,
  - террористического характера.

Приложение В
(справочное)

Факторы риска

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

Таблица В.1 — Опасности, источники и факторы риска

Наименование вида опасности	Фактор риска	Возможные источники
Механическая опасность	Физическое повреждение, травма, компрессионная асфиксия	Природные: землетрясения, оползни, сели, лавины, эрозия, обвалы, ураганы, наводнения. Техногенные: взрыв, авария, нарушение целостности конструкций, обрушение, затопление. Антропогенные: нападение, диверсия, терроризм
Опасность взрыва	Физическое повреждение, травма, ожог, компрессионная асфиксия	Природные: грозы, извержение вулканов Техногенные: авария, пожар, взрыв Антропогенные: поджог, осуществление взрыва, диверсии, инициирование аварии
Опасность пожара	Отравление продуктами горения, ожог, термическое повреждение, физическое повреждение, компрессионная асфиксия	Природные: грозы, извержение вулканов Техногенные: взрыв, пожар, короткое замыкание в электрических цепях, перегрев электронагревательных приборов Антропогенные: поджог, инициирование взрыва, аварии; нарушение правил пожарной безопасности
Термическая опасность	Термическое поражение	Природные: извержение вулканов Техногенные: аварии, нарушение технологических процессов (если процессы имеются); Антропогенные: инициирование аварии, диверсия
Опасность излучений (неионизирующих)	Поражение важных органов организма человека	Природные: солнечная радиация, извержение вулканов Техногенные: аварии, нарушение технологических режимов оборудования Антропогенные: инициирование аварий; нарушение технологических процессов
Биологическая опасность	Инфекционное заболевание	Природные: грибки, плесень Техногенные: нарушение режимов обращения, хранения, удаления биологических отходов; нарушение санитарных правил и норм Антропогенные: распространение патогенных микроорганизмов и вирусов; нарушение санитарных правил и норм
Промышленная опасность	Физическое повреждение, травма, ожог, компрессионная асфиксия	Природные: отсутствуют Техногенные: аварии, нарушение технологических процессов, взрывы, пожары, подтопление. Антропогенные: осуществление взрыва, поджога, диверсии; нарушение правил эксплуатации, правил пожарной безопасности, взрывобезопасности, правил пользования системами жизнеобеспечения

Окончание таблицы В.1

Наименование вида опасности	Фактор риска	Возможные источники
Химическая опасность	Химическое поражение	Природные: выбросы газов Техногенные: взрывы, аварии, утечка химически активных и ядовитых веществ Антропогенные: осуществление взрывов, диверсии; нарушение правил эксплуатации систем жизнеобеспечения
Электрическая опасность	Поражение электрическим током	Природные: удары молний Техногенные: аварии; нарушение работы электрооборудования, нарушение изоляции токонесущих цепей в результате взрыва, пожара, обрушения Антропогенные: осуществление взрывов, диверсии, поджогов; нарушение правил эксплуатации, правил электробезопасности, взрывобезопасности и пожарной безопасности
Радиационная опасность	Радиационное поражение организма человека	Природные: выбросы радона Техногенные: отсутствуют Антропогенные: распространение радиоактивных веществ; нарушение правил обращения с радиоактивными веществами
Ядерная опасность	Радиационное поражение, термическое поражение, ожог, физическое повреждение	Природные: отсутствуют Техногенные: отсутствуют Антропогенные: маловероятны
Антропогенная опасность	Механическое, химическое, радиационное, биологическое повреждение (заболевание), травма, ожог, отравление продуктами горения	Природные: отсутствуют Техногенные: возможны в отсутствие систем, связанных с безопасностью инженерного оборудования Антропогенные: нападение, диверсия, осуществление взрыва, поджога, инициирование аварии, распространение патогенных микроорганизмов и вирусов, ядовитых и радиоактивных веществ; нарушение правил эксплуатации, правил безопасности; ошибки оператора, ошибки пользователей

Приложение Г
(справочное)

Критерий и категории тяжести последствий

В качестве одного из критериев тяжести последствий при реализации опасных событий в зданиях и сооружениях может быть выбран вред, причиненный жизни и здоровью людей, пребывающих 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 0,3
3	Причинение вреда здоровью от 2 до 10 человек	До 3
4	Гибель одного человека	До 8,5
5	Гибель от 2 до 5 человек	До 42,5
6	Гибель до 10 человек	До 85
7	Гибель до 50 человек	До 450
8	Гибель до 300 человек	До 2 500
9	Гибель более 300 человек	Более 2 500

Приложение Д
(справочное)

Принцип разумной достаточности и приемлемого риска

Д.1 Модель разумной достаточности

В соответствии с принципом разумной достаточности ALARP[1)] требуется, чтобы любой риск был снижен, насколько это реально возможно и целесообразно. На рисунке Д.1 показаны три зоны риска. В зоне недопустимого риска риск не может быть оправдан ни при каких обычных обстоятельствах. Нижняя зона — зона явно приемлемого риска. Между этими зонами лежит зона разумной достаточности или зона приемлемости риска. В этой зоне допускается деятельность, если относящиеся к ней риски снижены настолько, насколько это реально возможно и целесообразно. В ней следует задавать уровень приемлемого риска и устанавливать уровень максимально допустимого риска.

В зоне явно приемлемого риска уровень риска настолько низок, что тем, кто управляет рисками, нет необходимости предоставлять доказательства, запрашивать разрешение (и ресурсы) для дальнейшего его снижения. Однако в этом случае следует следить за тем, чтобы риск оставался на этом уровне и не приближался к уровню максимально допустимого риска.

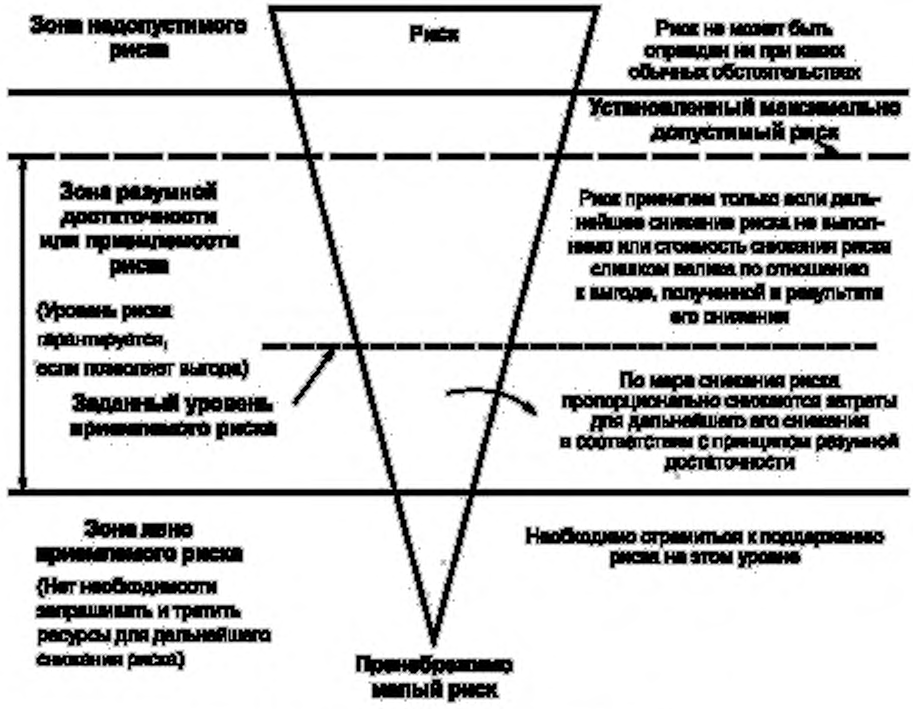


Рисунок Д.1 — Приемлемый риск и разумная достаточность

Модель разумной достаточности следует применять в случаях, когда планирование риска осуществляется с использованием количественного или качественного метода. Принцип применения количественного метода планирования риска описан в разделе Е.2 приложения Е, а принципы применения качественных методов для определения необходимого снижения риска для конкретного опасного события описаны в приложениях Ж и И.

[1)] Принцип разумной достаточности в стандарте [2] назван принципом ALARP. ALARP — это аббревиатура от английского «as low as reasonably practicable», означающая, «настолько низкий, насколько практически рационально» по отношению к уровню риска.

Д.2 Планирование допустимого риска

Для задания приемлемого риска может быть применен способ, состоящий в определении последствий в случае реализации опасных событий и назначении им приемлемых частот. Согласование последствий и приемлемых частот должно достигаться согласованием и выработкой компромиссного соглашения между заинтересованными сторонами (например, органами власти, осуществляющими техническое регулирование в области безопасности; теми, чья деятельность является источником рисков, например, застройщиками, владельцами объектов или лицами, управляющими объектами и теми, кто подвергается риску — эксплуатирующим персоналом, пользователями объектов, а также лицами, попадающими в зону действия объекта).

С учетом концепции разумной достаточности соответствие между последствиями опасных событий и частотами их появления может быть дано в виде классов риска. В таблице Д.1 для примера показано четыре класса рисков (I, II, III и IV) для ряда последствий и частот, в таблице Д.2 приведена возможная интерпретация последствий, а в таблице Д.3 дана интерпретация каждого из классов на основании рисунка Д.1. В определениях этих классов приняты риски после принятия мер по их снижению. В соответствии с рисунком Д.1 имеются следующие классы рисков:

I — в зоне недопустимого риска;

II и III — в зоне разумной достаточности, причем риск класса II находится у самой границы зоны разумной достаточности;

IV — в зоне явно приемлемого риска.

Для каждой конкретной ситуации должны быть разработаны таблицы, аналогичные таблице Д.1, с учетом социальных, политических и экономических факторов. Каждому последствию должна быть поставлена в соответствие частота возникновения события, и таблица должна быть заполнена классами риска. Например, частота в таблице Д.1 может обозначать частоту события (полученная на основании продолжительного опыта), которая могла бы быть заданной, как частота больше, чем 10 раз в год. Критерием последствий может служить причинение вреда жизни и здоровью людей.

Критическим последствием могла бы быть гибель одного человека и/или многочисленные серьезные повреждения нескольких людей, либо несколько профессиональных заболеваний (таблица Д.2).

Таблица Д.1 — Пример классификации рисков опасных событий

Частота опасных событий	Класс риска последствий опасных событий			
	катастрофические	критические	небольшие	несущественные
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 их появления, вероятности и т.п. Таблица служит примером того, как таблица должна заполняться, и не предназначена для прямого применения.

Таблица Д.2 — Возможная интерпретация последствий

Наименование последствия	Содержание последствия	Совокупный ущерб, млн. руб.
Катастрофические	Гибель большого числа людей (до 100 человек), заболевание до 1000 человек	Более 1 000
Критические	Гибель одного человека и/или многочисленные серьезные повреждения или заболевание до десяти человек	Более 8,0
Малые	Небольшая травма или заболевание одного человека	До 0,1
Несущественные	—	До 0,03

Таблица Д.3 — Интерпретация классов риска

Класс риска	Интерпретация класса риска
I	Недопустимый риск
II	Нежелательный риск, и допустимый только, если снижение риска не осуществимо или если затраты не чрезвычайно велики по сравнению с полученной выгодой
III	Приемлемый риск, если затраты на снижение риска не превышают полученную выгоду
IV	Пренебрежимо малый риск

Приложение Е
(справочное)

Определение уровней полноты безопасности: количественный метод

Е.1 Общие положения

Количественный метод применим, когда:

- допустимый риск может быть задан в числовой форме (например, определенное последствие не должно произойти чаще, чем $1 \cdot 10^{-4}$ лет);

- заданы числовые целевые (планируемые) значения полноты безопасности для СБЗС-систем. Такие целевые значения определены в ГОСТ Р 53195.2.

Метод, в частности, применим для моделей риска, показанных на рисунках Е.1, Е.2 настоящего приложения и рисунке Д.1 приложения Д.

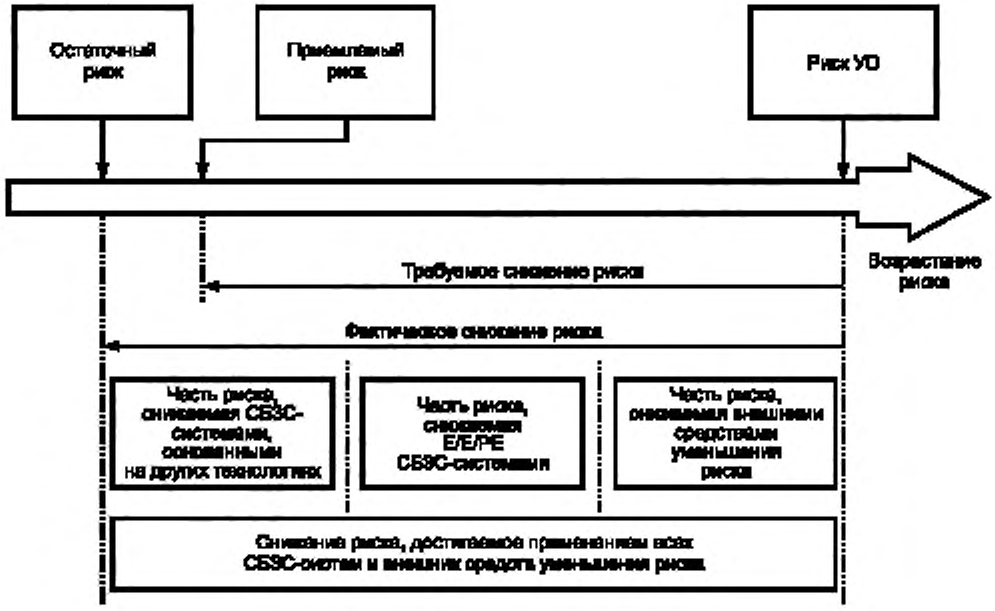


Рисунок Е.1 — Общий подход к снижению риска

В модели снижение риска УО до уровня приемлемого риска достигается применением внешних средств уменьшения риска и СБЗС-системам, каждая из которых снижает часть риска (рисунок Е.1). Снижение риска этими системами и средствами осуществляют с некоторым запасом, чтобы остаточный риск не превысил установленный максимально допустимый риск.

Снижение риска достигается выполнением функций безопасности, обеспечиваемых СБЗС-системами и внешними средствами уменьшения риска. Полнота их безопасности должна соответствовать требуемому снижению риска от начального риска УО до целевого приемлемого риска, который устанавливается при расчетах (рисунок Е.2).

Функция безопасности может быть распределена по нескольким системам, связанным с безопасностью (рисунок Е.3).Требования к полноте безопасности связываются с каждой функцией безопасности до распределения.

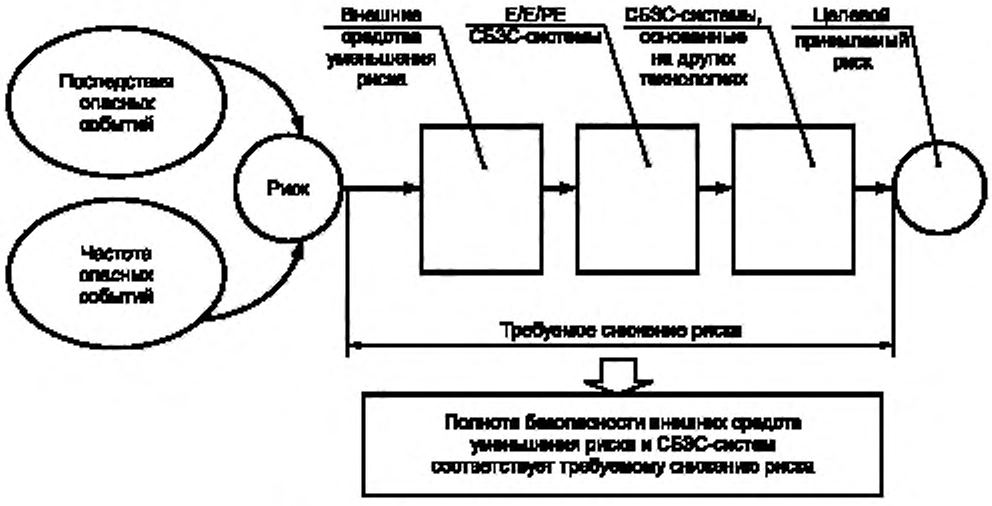


Рисунок Е.2 — Риск и полнота безопасности

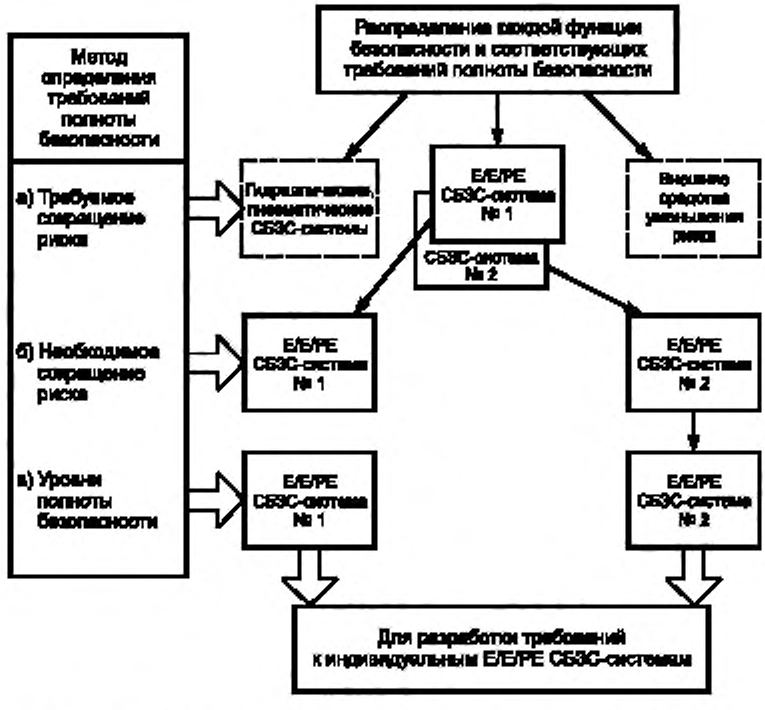


Рисунок Е.3 — Распределение требований безопасности по СБЗС-системам и внешним средствам уменьшения риска

Е.2 Основной метод

В этом методе для каждой функции безопасности, выполняемой каждой E/E/PE СБЗС-системой, необходимо:

- определить допустимый риск по таблице, аналогичной таблице Д.1 приложения Д, заполненной для конкретной опасности;

- определить риск управляемого оборудования;
- определить необходимое снижение риска для достижения приемлемого риска;
- распределить необходимое снижение риска по E/E/PE СБЗС-системам, СБЗС-системам, основанным на других (гидравлической, пневматической) технологиях, и внешним средствам уменьшения риска (см. подраздел 7.6 ГОСТ Р 53195.2).

Таблица Д.1, заполненная частотами возникновения опасных событий, приводящих к риску, позволяет определить целевой приемлемый риск F_t.

Частота опасных событий, связанная с риском, который существует для УО, включая систему управления УО и ошибки человека (риск УО), без каких-либо защитных средств, может быть оценена с использованием численных методов оценки риска. Частота, с которой может происходить опасное событие в отсутствие защитных средств $F_{пр}$, является одним из двух компонентов риска УО. Другой компонент риска — это последствие опасного события. $F_{пр}$ может быть определена с помощью:

- анализа частоты (интенсивности) отказов в сопоставимых ситуациях;
- данных из признанных баз данных;
- вычислений (расчетов) с применением соответствующих методов прогноза.

Е.3 Порядок расчета

Пример расчета целевой (планируемой) полноты безопасности для одиночной СБЗС-системы показан на рисунке Е.4. Для этого случая

$$PFD_{avg} \le F_t / F_{пр}, \qquad (Е.1)$$

где PFD_{avg} — средняя вероятность отказа E/E/PE СБЗС-системы при выполнении операции по запросу, работающей в режиме с низкой частотой запросов (см. таблицу 2 ГОСТ Р 53195.2),

F_t — частота для приемлемого риска,

$F_{пр}$ — частота запросов к E/E/PE СБЗС-системе.

На рисунке Е.4 также обозначены:

C — последствие опасного события,

F_p — частота для риска при установленной E/E/PE СБЗС-системе,

ΔR — необходимое снижение риска.

Определение $F_{пр}$ для УО важно из-за его связи с PFD_{avg} и, следовательно, с уровнем полноты безопасности СБЗС-системы.

Для получения уровня полноты безопасности (при неизменном последствии, как на рисунке Е.4) для ситуации, когда все необходимое снижение риска достигается одиночной СБЗС-системой, которая должна уменьшить частоту опасных событий, как минимум, с $F_{пр}$ до F_t, необходимо:

- определить частоту событий риска УО в отсутствие каких-либо средств защиты ($F_{пр}$);
- определить последствие C в отсутствие каких-либо средств защиты;
- определить, с использованием таблицы Д.1, достигается ли для частоты $F_{пр}$ и последствия C уровень приемлемого риска. Если на основании таблицы Д.1 получен класс риска I, то требуется дальнейшее снижение риска. Риски классов IV или III могут быть приняты как приемлемые риски. Риск класса II требует дальнейшего изучения.

Примечание — Таблица Д.1 используется для проверки, требуются ли дальнейшие меры по снижению риска.

- определить среднюю вероятность отказа СБЗС-системы при работе по запросу (PFD_{avg}), состоящего в невозможности достичь необходимого снижения риска (ΔR). Для постоянного последствия в описанной конкретной ситуации, $PFD_{avg} = (F_t / F_{пр}) = \Delta R$;
- определить из таблицы 2 ГОСТ Р 53195.2 уровень полноты безопасности для $PFD_{avg} = (F_t / F_{пр})$ (например, для $PFD_{avg} = 10^{-2} — 10^{-3}$ уровень полноты безопасности равен SIL 2).

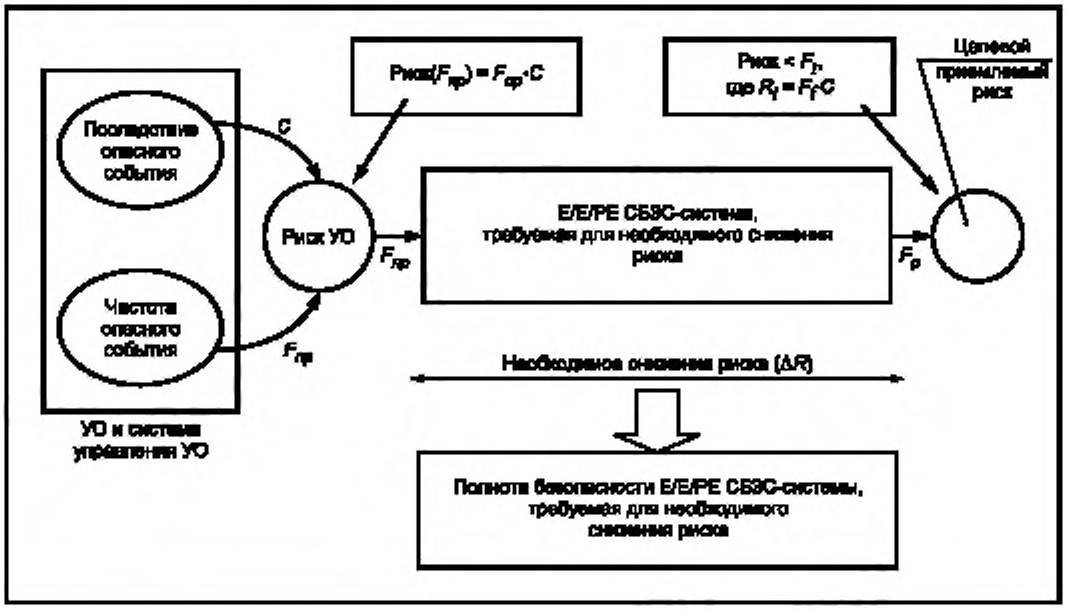


Рисунок Е.4 — Схема расчета целевой полноты безопасности одиночной E/E/PE СБЗС-системы

Приложение Ж
(справочное)

Определение уровней полноты безопасности: качественный метод

Ж.1 Общие положения

При использовании графического качественного метода (графа риска) следует ввести ряд параметров, которые в совокупности описывают природу опасной ситуации, если СБЗС-система отказывает или находится вне доступа. Из каждого из четырех наборов выбирают один параметр, выбранные параметры объединяют, чтобы вынести решение о распределении полноты безопасности по СБЗС-системам. Эти параметры позволяют осуществить градуировку рисков, поддающейся интерпретации, и содержат ключевые факторы оценки риска.

Приложение не предназначено для окончательных расчетов этим методом, а служит для иллюстрации основных принципов его применения.

Ж.2 Синтез графа риска

Приведенные ниже упрощенные процедуры определения уровня полноты безопасности основаны на выражении

$$R = f \cdot C, \qquad (Ж.1)$$

где R — риск в отсутствие СБЗС-системы;

f — частота опасного события в отсутствие СБЗС-системы;

C — последствия опасного события (последствия должны быть отнесены к причинению вреда жизни и здоровью людей).

Частота опасных событий f в этом случае определяется тремя влияющими факторами:

- частотой и временем пребывания в опасной зоне;
- вероятностью избегания опасного события;
- вероятностью наступления опасного события в отсутствие какой-либо СБЗС-системы (но при наличии внешних средств уменьшения риска), называемой вероятностью нежелательного события.

Следствием частоты являются четыре следующих параметра:

- последствие опасного события C;
- частота и время воздействия в опасной зоне F;
- вероятность неудачи в избегании опасного события P;
- вероятность нежелательного случая W.

Ж.3 Другие возможные параметры риска

Полагается, что определенные выше параметры риска являются в достаточной степени родовыми, чтобы их можно было распространять на широкий диапазон применений. Однако возможны случаи, когда требуется введение дополнительных параметров, например, при использовании новых технических средств в УО и в системах управления УО. Введение дополнительных параметров способствует более точной оценке необходимого снижения риска.

Ж.4 Реализация графа риска: общая схема

Качественный метод графа риска может быть применен, когда модель риска соответствует модели, приведенной на рисунках Е.1 и Е.2 приложения Е. Он позволяет определить уровень полноты безопасности E/E/PE СБЗС-системы, исходя из знаний факторов риска, связанных с УО и системой управления УО.

Комбинация описанных выше параметров риска позволяет получить граф риска в виде, показанном на рисунке Ж.1, где $C_A < C_B < C_C < C_D$; $F_A < F_B$; $P_A < P_B$; $W_1 < W_2 < W_3$.

Толкование этого графа риска следующее:

- Использование параметров риска C, F и P приводит к ряду исходов (выходов) $X_1, X_2, X_3, \ldots X_n$. Точное число выходов зависит от конкретной области применения и выбирается так, чтобы это применение было охвачено графом риска. На рисунке Ж.1 показана ситуация, при которой не вносится никакой дополнительный вклад для более серьезных последствий. Каждый из этих исходов (выходов) отображается на одной из трех шкал (W_1, W_2 или W_3). Каждая точка этих шкал обозначает необходимую полноту безопасности, которая должна быть достигнута с помощью рассматриваемой E/E/PE СБЗС-системы.

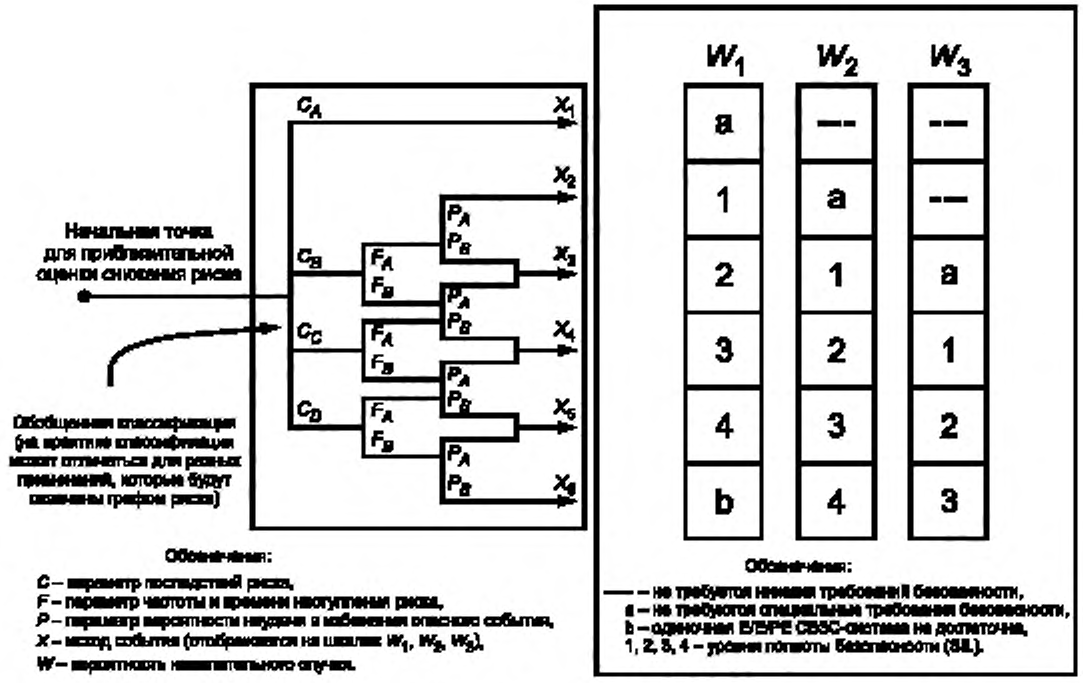


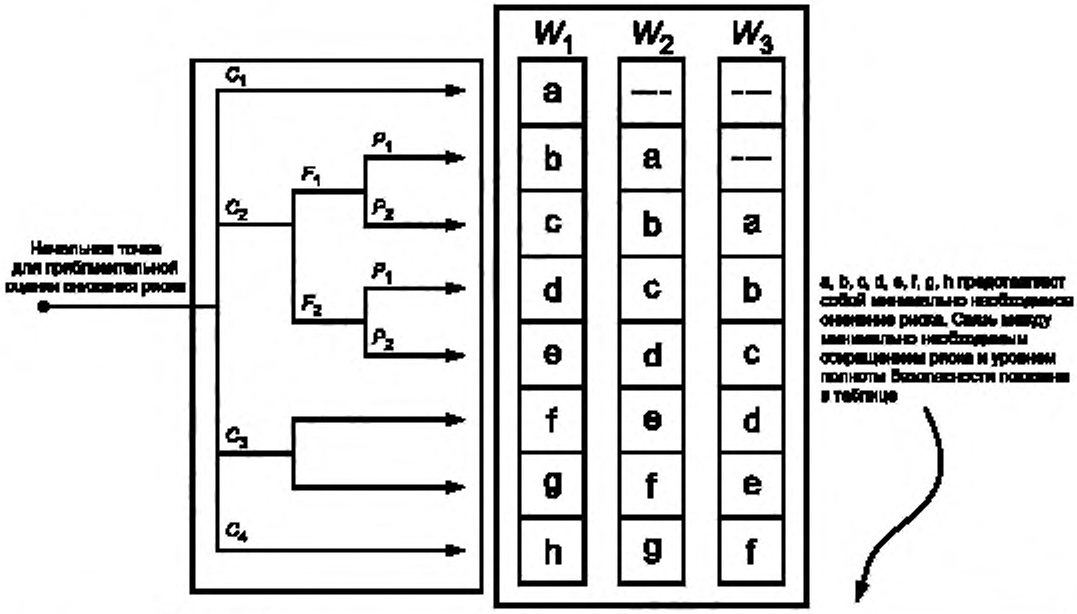
Рисунок Ж.1 — Общая схема графа риска

- Когда для конкретных последствий применение одиночной E/E/PE СБЗС-системы не достаточно, отображение на шкалах W_1, W_2 или W_3 позволяет использовать другие меры снижения риска. В этом случае, шкала W_3 означает минимальное снижение риска, внесенное другими средствами (то есть, самую высокую вероятность имеющего место нежелательного случая); шкала W_2 означает средний вклад, а шкала W_1 — максимальный вклад. Для конкретных промежуточных точек графа риска (например, X_1, X_2... или X_6) или для конкретной шкалы W (например, W_1, W_2 или W_3) окончательный исход (выход) графа риска дает уровень полноты безопасности E/E/PE СБЗС-системы (например, SIL1, SIL2, SIL3 или SIL4) и требуемое значение снижения риска для этой системы. Это снижение риска, вместе со снижением риска, достигаемым с помощью других средств (например, с помощью СБЗС-систем, основанных на гидравлических или пневматических технологиях, и внешних средств уменьшения риска), которые принимаются в расчет с помощью механизма W-шкал, дает необходимое снижение риска для конкретной ситуации.

Параметры, обозначенные на рисунке Ж.1 (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3), и их содержимое должны быть точно определены для каждой конкретной ситуации.

Ж.5 Пример графа риска

Реализация графа риска с использованием данных, отображенных на рисунке Ж.1, показана на рисунке Ж.2.



Минимально необходимое снижение риска	Требования к полноте безопасности
—	Требования отсутствуют
a	Специальные требования отсутствуют
b, c	SIL 1
d	SIL 2
e, f	SIL 3
g	SIL 4
h	E/E/PE СБЗС-системы не достаточно

Рисунок Ж.2 — Пример реализации графа риска

Использование параметров риска *C*, *F*, и *P* приводит к одному из восьми исходов (выходов). Каждый из этих исходов (выходов) обозначается на одной из трех шкал (W_1, W_2 и W_3). Каждая точка на этих шкалах (a, b, c, d, e, g и h) обозначает необходимое снижение риска, которое должно быть достигнуто СБЗС-системой.

Детализация данных, показанных на рисунке Ж.2, приведена в таблице Ж.1.

Таблица Ж.1 — Детализация данных к примеру графа риска

Наименование параметра риска	Обозначение параметра риска	Описание параметра риска	Примечание
Последствия *C*	C_1	Несущественный вред	Последствия рассмотрены для случаев причинения вреда здоровью и жизни людей. Для случаев причинения вреда окружающей среде или имуществу должны быть разработаны другие варианты классификации последствий Для интерпретации C_1, C_2, C_3 и C_4 должны быть приняты во внимание случаи катастроф и обычного оказания помощи (спасения)
	C_2	Серьезный долговременный вред, причиненный одному лицу или нескольким лицам; гибель одного человека	
	C_3	Гибель нескольких человек	
	C_4	Гибель очень большого числа людей	

Окончание таблицы Ж.1

Наименование параметра риска	Обозначение параметра риска	Описание параметра риска	Примечание
Частота и время воздействия опасности в опасной зоне F	F_1 F_2	От редкого до более частого подтверждения опасности в опасной зоне Частое или непрерывное подтверждение опасности в опасной зоне	Частота и время воздействия опасности рассмотрены для случаев причинения вреда здоровью и жизни людей. Для случаев причинения вреда окружающей среде или имуществу могут быть разработаны другие варианты классификации частоты и времени воздействия
Вероятность избежания опасного события P	P_1 P_2	Возможно при некоторых условиях Почти невозможно	Параметр учитывает: режим процесса (контролируемый квалифицированным или неквалифицированным лицом, неконтролируемый); скорость развития опасного события (неожиданно, быстро или медленно); легкость распознавания опасности (обнаруживается немедленно, обнаруживается техническими средствами, обнаруживается без технических средств); возможность избежать опасное событие, например, спасаясь бегством (не возможно или возможно при некоторых условиях); имеющийся практический опыт обеспечения безопасности (опыт может иметь место при использовании аналогичного УО или похожего УО, либо может отсутствовать)
Вероятность нежелательных случаев W	W_1	Очень небольшая вероятность того, что нежелательный случай произойдет; возможно лишь несколько нежелательных случаев	Цель применения W-фактора состоит в приблизительной оценке частоты появления нежелательного случая без применения каких-либо СБЗС-систем (E/E/PE-систем или систем, основанных на других технологиях), но с использованием любых внешних средств уменьшения риска
Вероятность нежелательных случаев W	W_2 W_3	Небольшая вероятность того, что нежелательный случай произойдет; возможно несколько нежелательных случаев Относительно высокая вероятность того, что нежелательный случай произойдет; возможны частые нежелательные случаи	Если опыт применения УО, систем управления УО, или подобных применяемым УО и системам управления УО невелик или отсутствует, приблизительная оценка W-фактора может быть сделана путем расчета. В этом случае должен быть использован наихудший прогноз

Приложение И
(справочное)

Определение уровней полноты безопасности — качественный метод: матрица критичности опасных событий

И.1 Общие положения

Качественный метод матрицы критичности опасных событий целесообразно применять, кода риск или частота его появления не могут быть определены количественно. Метод позволяет определять уровень полноты безопасности E/E/PE СБЗС-системы на основании знаний факторов риска, связанных с управляемым оборудованием и системой управления УО. Метод применим в случаях, когда модель риска аналогична модели, показанной на рисунках Е.1 и Е.2 приложения Е.

В настоящем методе предполагается, что каждая СБЗС-система и внешние средства уменьшения риска являются независимыми.

И.2 Матрица критичности опасных событий

В основу матрицы должны быть положены обязательные условия:

а) E/E/PE СБЗС-системы, СБЗС-системы, основанные на гидравлических или пневматических технологиях, и внешние средства уменьшения риска, являются независимыми;

б) СБЗС-системы и внешние средства уменьшения риска рассматриваются как слои защиты, которые обеспечивают частичные сокращения риска, как показано на рисунке Е.1 приложения Е.

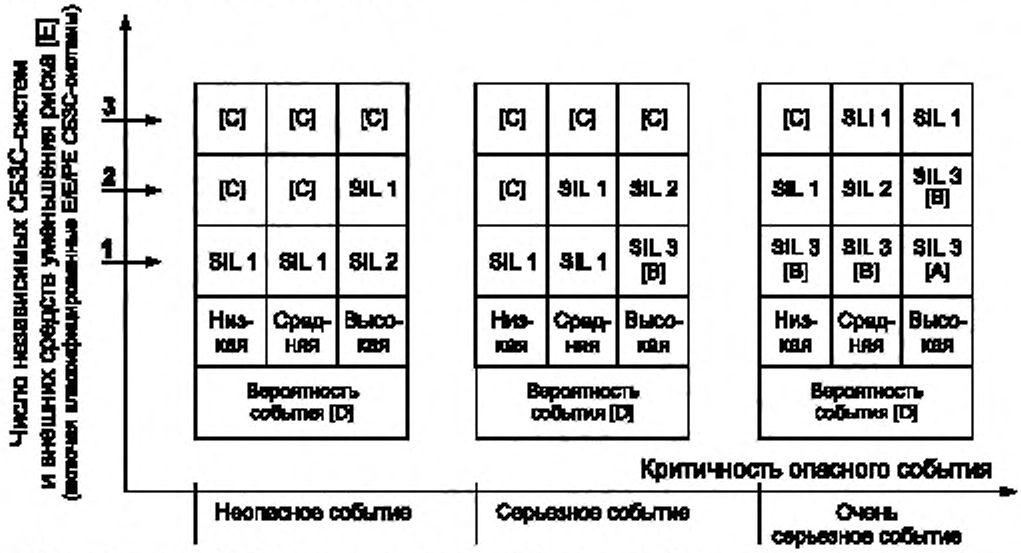
Примечание — Для выполнения этого условия требуется выполнение регулярных контрольных испытаний слоев защиты.

в) увеличение уровня полноты безопасности достигается тогда, когда добавляется один слой защиты — перечисление б);

г) используется только одна E/E/PE СБЗС-система, но она может быть объединена с СБЗС-системой, основанной на гидравлической или пневматической технологии, и/или с внешним средством уменьшения риска.

Эти требования распространяются на матрицу критичности опасных событий, показанную на рисунке И.1.

Матрица заполнена примерными данными для иллюстрации общих принципов. Для каждой конкретной ситуации должна быть построена своя матрица.



[A] — одиночная E/E/PE СБЗС-система с уровнем полноты безопасности SIL 3, которая не обеспечивает достаточное снижение риска на этом уровне риска (требуются дополнительные меры по снижению риска);

[B] — одиночная E/E/PE СБЗС-система с уровнем полноты безопасности SIL 3, которая может не обеспечить достаточное снижение риска на этом уровне риска (требуется анализ опасностей и риска для определения необходимости применения дополнительных мер по снижению риска);

[C] — независимая связанная с безопасностью E/E/PE СБЗС-система не требуется;

[D] — вероятность опасного события в отсутствие каких-либо СБЗС-систем или внешних средств уменьшения риска;

[E] — независимая E/E/PE СБЗС-система (вероятность события и суммарное число независимых слоев защиты определяется в соответствии с конкретным применением).

Рисунок И.1 — Матрица критичности опасных событий

Библиография

[1] МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины, определения, сокращения
IEC 61508-4:1998 Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 4: Definitions and abbreviations
[2] МЭК 61508-5:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности
IEC 61508-5:1998 Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels
[3] Руководство ИСО/МЭК 51:1999 Аспекты безопасности. Руководящие указания по включению их в стандарты
ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards

УДК 621.5:814.8:006.354	ОКС 13.100; 13.110; 13.220; 13.320	Ж20	ОКП 43 7000 43 7100 43 7200 43 7280 70 3000

Ключевые слова: безопасность функциональная; связанные с безопасностью зданий и сооружений системы; основные положения

Редактор *Н. О. Грач*
Технический редактор *Н. С. Гришанова*
Корректор *С. И. Фирсова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 10.03.2009. Подписано в печать 29.04.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 4,18. Уч.-изд. л. 3,30. Тираж 253 экз. Зак. 440.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru)@gostinfo. ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru