ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53195.2— 2008

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 2

Общие требования

Издание официальное

БЗ 8—2008/205

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. № 654-ст

4 В настоящем стандарте учтены 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 61508-1:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования» (IEC 61508-1:1998 Functional safety of electrical/ electronic/ programmable electronic safety-related systems — Part 1: General requirements);
- 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 . . . 3
5 Требования . . . 3
5.1 Соответствие системы требованиям стандарта . . . 3
5.2 Требования к документации . . . 3
6 Управление функциональной безопасностью . . . 4
7 Требования к полному жизненному циклу систем . . . 5
7.1 Общие положения . . . 5
7.2 Разработка концепции (см. блок 1 на рисунке 1). . . . 7
7.3 Определение области применения (см. блок 2 на рисунке 1) . . . 7
7.4 Анализ опасностей и риска (см. блок 3 на рисунке 1) . . . 8
7.5 Определение требований к функциям безопасности (см. блок 4 на рисунке 1) . . . 9
7.6 Распределение требований безопасности (см. блок 5 на рисунке 1) . . . 9
7.7 Разработка проектной документации на СБЗС-системы (см. блок 6 на рисунке 1) . . . 12
7.8 Разработка рабочей документации (см. блок 7 на рисунке 1) . . . 13
7.9 Планирование полной установки, интеграции и ввода в действие (см. блок 8 на рисунке 1) . . . 14
7.10 Планирование подтверждения соответствия систем требованиям функциональной безопасности (см. блок 9 на рисунке 1) . . . 15
7.11 Планирование эксплуатации и технического обслуживания систем (см. блок 10 на рисунке 1) 16
7.12 Реализация: E/E/PE СБЗС-систем (см. блок 11 на рисунке 1) . . . 16
7.13 Реализация СБЗС-систем, основанных на других технологиях (см. блок 12 на рисунке 1) . . . 17
7.14 Реализация внешних средств уменьшения риска (см. блок 13 на рисунке 1) . . . 17
7.15 Подтверждение соответствия (см. блок 14 на рисунке 1) . . . 17
7.16 Эксплуатация, техническое обслуживание, ремонт, периодический контроль (см. блок 15 на рисунке 1) . . . 17
7.17 Видоизменение и модификация (см. блок 16 на рисунке 1) . . . 19
7.18 Вывод из эксплуатации и утилизация (см. блок 17 на рисунке 1) . . . 21
7.19 Верификация E/E/PE СБЗС-систем . . . 22
8 Оценка функциональной безопасности . . . 22
Приложение А (справочное) Перечень и идентификация документации . . . 25
Приложение Б (справочное) Пример структуры документации . . . 28
Приложение В (справочное) Компетентность лиц . . . 29

Введение

Современное здание или сооружение — объект строительного производства представляет собой сложную систему, включающую систему конструкций и разные сочетания систем, в том числе инженерных систем жизнеобеспечения, реализации процессов, энерго-, ресурсосбережения, безопасности и других систем. Эти системы взаимодействуют друг с другом, с внешней и внутренней средой.

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, мероприятий и средств для снижения риска причинения вреда до уровня приемлемого риска и поддержания этого уровня в течение периода эксплуатации или использования объектов. К техническим средствам снижения риска относятся системы, связанные с безопасностью зданий и сооружений. Эти системы, состоящие из электрических и/или электронных компонентов, 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 обеспечения безопасности зданий и сооружений во все больших объемах используются программируемые электронные, т. е. компьютерные системы.

Стандарт устанавливает общие требования к документации, управлению функциональной безопасностью, оценке функциональной безопасности связанных с безопасностью зданий и сооружений систем (СБЗС-систем). В настоящем стандарте установлены общие требования к полному жизненному циклу СБЗС-систем, отдельным его стадиям, и определены основные целевые уровни полноты безопасности функций безопасности, которые должны быть реализованы СБЗС-системами.

Настоящий стандарт рассчитан на полный диапазон технологической сложности СБЗС-систем и ориентирован на комплексное обеспечение безопасности объектов.

Настоящий стандарт входит в комплекс стандартов с наименованием «Безопасность функциональная связанных с безопасностью зданий и сооружений систем» (Часть 2 — Общие требования). Другие стандарты, входящие в этот комплекс:

Часть 1. Основные положения

Часть 3. Требования к системам

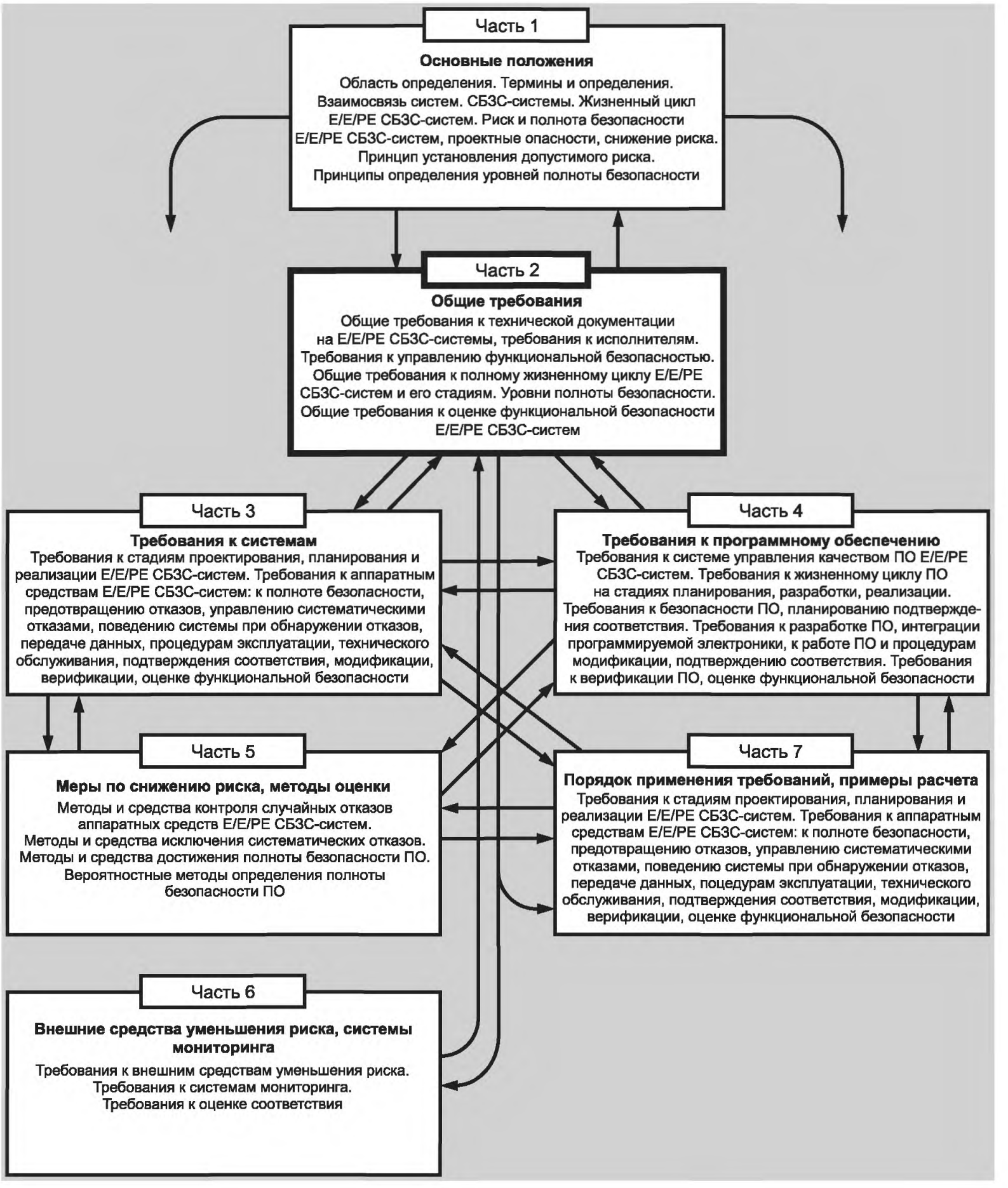
Часть 4. Требования к программному обеспечению

Часть 5. Меры по снижению риска, методы анализа риска и оценки полноты безопасности

Часть 6. Внешние средства уменьшения риска и системы мониторинга конструкций

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

Структура комплекса стандартов приведена ниже.



НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ СИСТЕМ

Часть 2

Общие требования

Functional safety of building/erection safety-related systems.
Part 2. General requirements

Дата введения — 2010—01—01

1 Область применения

Настоящий стандарт распространяется на электрические, электронные, программируемые электронные (E/E/PE) СБЗС-системы, устанавливаемые и установленные во вновь возводимых или реконструируемых зданиях и сооружениях.

Настоящий стандарт устанавливает общие требования к документации, к управлению функциональной безопасностью E/E/PE СБЗС-систем, к функциональной безопасности этих систем на всех стадиях их жизненного цикла, а также к действиям на этих стадиях, обеспечивающим функциональную безопасность.

Настоящий стандарт не распространяется на связанные с безопасностью зданий и сооружений системы, в которых E/E/PE СБЗС-система является одиночной системой, способной осуществить необходимое снижение риска, и требуемая полнота безопасности такой системы ниже, чем определено уровнем полноты безопасности SIL1 — самым низким уровнем полноты безопасности, определенным в таблицах 1 и 2 настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 21.1703—2000 Система проектной документации для строительства. Правила выполнения рабочей документации проводных средств связи

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

ГОСТ Р 53195-1—2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения

ГОСТ 2.102—68 Единая система конструкторской документации. Виды и комплектность конструкторских документов

ГОСТ 2.610—2006 Единая система конструкторской документации. Правила выполнения эксплуатационных документов

ГОСТ 21.101—97 Система проектной документации для строительства. Основные требования к проектной документации

ГОСТ 21.501—93 Система проектной документации для строительства. Правила выполнения архитектурно-строительных рабочих чертежей

Издание официальное

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.

3 Термины и определения

В настоящем стандарте применены термины, сокращения и обозначения, приведенные в ГОСТ Р 53195.1, а также термины, приведенные ниже.

3.1 **независимая организация** (independent organization): Отдельная организация, выполняющая оценку и аудит функциональной безопасности, не имеющая общего управления и ресурсов с организациями, ответственными за процессы, осуществляемые в течение конкретной стадии жизненного цикла связанной с безопасностью зданий и сооружений системы или программного обеспечения.

3.2 **независимое лицо** (independent person): Лицо, проводящее оценку и аудит функциональной безопасности, не зависимое и не связанное с действиями, происходящими во время конкретной стадии жизненного цикла связанной с безопасностью системы или ее составляющей и не несущее прямой ответственности за эти действия.

3.3 **независимое подразделение** (independent department): Подразделение, которое выполняет оценку или аудит функциональной безопасности, не зависимое и не связанное с подразделениями, отвечающими за действия, осуществляемые в течение конкретной стадии жизненного цикла связанной с безопасностью системы или ее составляющей, либо программного обеспечения.

3.4 **режим работы связанной с безопасностью системы;** режим работы СБС (operate mode of safety-related system): Режим работы связанной с безопасностью системы, характеризующийся частотой запросов к ней, который может быть либо режимом с низкой частотой запросов, когда частота обращений для выполнения операции, связанной с безопасностью системой, не превышает одного раза в год или не превышает более чем в два раза частоту, зарегистрированную во время контрольных испытаний, либо режимом с высокой частотой запросов или непрерывным запросом, когда частота запросов превышает более чем в два раза частоту, зарегистрированную во время контрольных испытаний.

3.5 **полная функция безопасности** (overall safety function): Функция безопасности программируемой электронной связанной с безопасностью системы, обеспеченная одновременным действием аппаратных средств и программного обеспечения этой системы.

3.6 **связанное с безопасностью зданий и сооружений программное обеспечение;** СБЗС ПО: Программное обеспечение, которое используется для реализации функций безопасности в связанных с безопасностью зданий и сооружений системах.

3.7 **управление конфигурацией** (configuration management): Процесс идентификации компонентов рассматриваемых систем, управления изменением этих компонентов, связей между ними, поддержания преемственности и сопровождения на протяжении всего их жизненного цикла.

3.8 **уровень полноты безопасности программного обеспечения;** уровень полноты безопасности ПО (software SIL): Дискретный уровень, принимающий одно из четырех возможных значений, определяющий полноту безопасности программного обеспечения связанной с безопасностью системы.

Примечание — Уровень полноты безопасности SIL4 характеризует наибольшую полноту безопасности программного обеспечения, уровень SIL1 соответствует наименьшей полноте безопасности программного обеспечения.

3.9 **целевая величина отказов** (target failure measure): Целевая вероятность опасных отказов в опасном режиме, которая должна быть достигнута в соответствии с требованиями к полноте безопасности.

Примечание — Целевая величина отказов выражается в виде средней вероятности опасного отказа при выполнении запроектированной функции безопасности по запросу — для режима работы с низкой частотой запросов или вероятности возникновения опасных отказов в течение часа — для режима с высокой частотой запросов или непрерывными запросами.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и обозначения.

АР — архитектурное решение проекта,

АС — архитектурно-строительное решение проекта,

СБЗС ПО — связанное с безопасностью зданий и сооружений программное обеспечение;

международные обозначения:

H — режим работы системы с высокой частотой запросов или непрерывным запросом,

L — режим работы системы с низкой частотой запросов.

5 Требования

5.1 Соответствие системы требованиям стандарта

E/E/PE СБЗС-система признается соответствующей требованиям настоящего стандарта, если представлены доказательства удовлетворения требований и достижения всех целей, установленных в настоящем стандарте.

Примечания

1 В качестве доказательных материалов следует использовать выходные данные, подлежащие документированию, предусмотренные в разделе 7 настоящего стандарта, верифицированные в соответствии с 7.19 и содержащие результаты оценки функциональной безопасности, проведенной в соответствии с разделом 8.

2 На стадиях проектирования, сдачи в эксплуатацию, эксплуатации и видоизменения (модификации) СБЗС-систем лицам, ответственным за безопасность на соответствующей стадии или стадиях, по их запросу должна быть представлена информация, предусмотренная 7.7, 7.15, 7.16, 7.17, 7.19.

3 В настоящем стандарте учтены положения руководства ИСО/МЭК 51 [1] по аспектам безопасности и требования стандартов ГОСТ Р ИСО 9000, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 9004 по системам менеджмента качества и улучшению деятельности.

5.2 Требования к документации

5.2.1 Документированию подлежит информация, необходимая для реализации всех стадий полного жизненного цикла СБЗС-систем и программного обеспечения этих систем, в том числе информация, требуемая для осуществления: управления функциональной безопасностью, верификации, действий по обеспечению функциональной безопасности и ее оценки.

Примечание — Документацию допускается представлять на бумаге или в электронной форме на носителе записи в виде, пригодном для отображения на экранах или дисплеях.

5.2.2 В состав проектной и рабочей документаций должна быть включена документация, указанная в Градостроительном кодексе Российской Федерации, предусмотренная ГОСТ Р 21.1703, ГОСТ 21.101, ГОСТ 2.102, ГОСТ 21.501, ГОСТ 2.610, сводами правил по назначению объектов, имеющая положительное заключение государственной экспертизы и утвержденная застройщиком или заказчиком, а также документация, предусмотренная настоящим стандартом.

5.2.3 В комплект документации на особо опасные, технически сложные и уникальные строительные объекты должен входить раздел проекта «Мероприятия по комплексному обеспечению безопасности» и комплект рабочей графической и текстовой документации на систему комплексного обеспечения безопасности зданий и сооружений, содержащий требования и сведения, необходимые для комплексного обеспечения безопасности и антитеррористической защищенности объекта в соответствии с требованиями утвержденных в установленном порядке технических условий (специальных технических условий) и технического задания на проектирование объекта, а также для оценки соответствия.

5.2.4 В технических условиях (специальных технических условиях) и/или в задании на проектирование здания и сооружения должны быть установлены проектные опасности и угрозы, модели нарушителей, требования к системе комплексного обеспечения безопасности объекта с применением СБЗС-систем в зависимости от особенностей, степени ответственности, категории опасности объекта и местных условий.

Приложение — Перечень основных СБЗС-систем и/или подсистем, входящих в комплексную систему безопасности объекта, приведен в ГОСТ Р 53195.1 (раздел А.2 приложения А).

5.2.5 Состав и число СБЗС-систем или подсистем для комплексного обеспечения безопасности конкретного здания или сооружения в соответствии с требованиями утвержденных в установленном порядке технических условий и технического задания определяются на стадии проектирования.

5.2.6 Документация, относящаяся к СБЗС-системам, со всеми утвержденными изменениями должна быть сохранена на протяжении всего жизненного цикла систем и объекта. Она должна соответствовать перечисленным ниже требованиям.

5.2.7 Документация должна содержать информацию для каждой стадии полного жизненного цикла СБЗС-систем и их составляющих (циклов E/E/PE СБЗС-систем и их программного обеспечения), достаточную для реализации составляющих стадий и действий по верификации в соответствии с 7.19, управлению функциональной безопасностью в соответствии с разделом 6, оценке функциональной безопасности в соответствии с разделом 8, а также информацию и результаты, полученные от любой иной оценки функциональной безопасности.

5.2.8 Документации должны быть присвоены идентификационные признаки: наименование, отображающее область применения содержимого, индекс классификации (или маркировка), обеспечивающий доступ к информации, предусмотренный настоящим стандартом, индекс пересмотра или номер версии для обеспечения возможности идентификации различных версий документа.

5.2.9 Документация должна быть структурирована таким образом, чтобы обеспечить возможность лицам, осуществляющим действия, связанные с обеспечением безопасности на стадиях жизненного цикла E/E/PE СБЗС-систем, поиска существенной информации. Документация должна быть скомпонована в комплекты, удобные для пользования этими лицами (см. приложение Б).

Примечания

1 Структура документации может изменяться в зависимости от состава, числа E/E/PE СБЗС-систем, их сложности и организационных требований.

2 Рекомендуемые к применению перечень и идентификация проектной и рабочей документации и документации, выпускаемой на других стадиях жизненных циклов E/E/PE СБЗС-систем, приведены в приложении А.

5.2.10 Проверка, изменения, пересмотр, утверждение документации должны быть обеспечены соответствующей системой управления документацией.

6 Управление функциональной безопасностью

6.1 Управление и технические действия организаций (отделов, лиц), ответственных за безопасность E/E/PE СБЗС-систем, должны быть направлены на поддержание требуемой полноты безопасности в течение полного жизненного цикла систем.

6.2 Организации (отделы, лица), несущие ответственность за одну или несколько стадий жизненного цикла E/E/PE СБЗС-систем, их аппаратных средств или программного обеспечения, должны определить все управленческие и технические действия, которые необходимы для достижения и поддержания СБЗС-системами требуемой функциональной безопасности, и разработать планы мероприятий, в которых должны быть учтены:

- техническая политика и стратегия по достижению функциональной безопасности, методы ее оценки, мероприятия по ее достижению и средства, с помощью которых осуществляется взаимодействие внутри организации для обеспечения высокого качества работ в области безопасности;
- идентификация лиц, отделов и организаций, ответственных за осуществление и контроль примененных стадий жизненного цикла E/E/PE СБЗС-систем, аппаратных средств или программного обеспечения, включая, при необходимости, идентификацию авторизованных лицензий и органов регулирования, выдавших эти лицензии;
- стадии полного жизненного цикла E/E/PE СБЗС-систем, аппаратных средств или программного обеспечения, которые должны быть применены;
- способ структурирования и объем информации, подлежащей документированию, в соответствии с 5.2;
- выбранные средства и оборудование, используемые для удовлетворения требований;
- действия по оценке функциональной безопасности, в соответствии с требованиями раздела 8;
- процедуры по обеспечению быстрого исполнения рекомендаций и решений, относящихся к E/E/PE СБЗС-системам, принятых в результате:
- анализа опасностей и рисков в соответствии с 7.4;
- оценки функциональной безопасности в соответствии с разделом 8;
- действий по верификации, установленных в 7.19;
- действий по подтверждению соответствия, установленных в 7.10 и 7.15;
- видоизменений и модификаций в соответствии с 7.17;

- процедуры, гарантирующие компетентность лиц, вовлеченных в действия по обеспечению жизненного цикла E/E/PE СБЗС-систем, аппаратных средств или программного обеспечения, а именно:
- обучение и тренинг персонала в части диагностирования отказов, ремонта и тестирования систем;
- обучение и тренинг персонала операторов;
- периодическая переподготовка персонала (см. приложение В);
- процедуры, удостоверяющие проведение анализа опасных и потенциально опасных событий и подготовку рекомендаций по минимизации вероятности их повторения;
- процедуры по анализу действий и поддержанию рабочих характеристик системы, в том числе процедуры:
- распознавания систематических отказов, подвергающих риску функциональную безопасность, включая процедуры обнаружения повторных отказов, используемые в течение обычной эксплуатации;
- оценки соответствия частоты запросов и частоты или интенсивности отказов во время работы требованиям, принятым при разработке системы;
- требования к периодической проверке функциональной безопасности в соответствии с настоящим подразделом, в том числе:
- к частоте проверок функциональной безопасности;
- к уровню независимости, требуемому для лиц, отделов, организаций, ответственных за проверки;
- к документированию и исполнению действий;
- процедуры по инициированию модификаций E/E/PE СБЗС-систем в соответствии с 7.17;
- процедуры по согласованию и утверждению модификаций;
- процедуры по поддержанию точной информации о потенциальных опасностях и СБЗС-системах;
- процедуры по управлению конфигурацией E/E/PE СБЗС-систем в течение стадий их полного жизненного цикла и жизненных циклов аппаратных средств и программного обеспечения; в частности должно быть установлены:
- стадия, на которой должен быть осуществлен формальный контроль конфигурации;
- процедуры, которые используются для уникальной идентификации всех составляющих частей E/E/PE СБЗС-систем, аппаратных средств и программного обеспечения;
- процедуры, препятствующие прониканию на объект неавторизованных частей систем, поступивших от служб технического обслуживания;
- условия обучения и информация для служб безопасности и служб спасения (МЧС, неотложной медицинской помощи, безопасности и правопорядка), в случае необходимости.

6.3 Мероприятия, разработанные в соответствии с требованиями 6.2, должны быть рассмотрены заинтересованными организациями и согласованы. Организации, с которыми должны быть согласованы мероприятия, должны быть установлены в технических условиях (специальных технических условиях) и/или задании на проектирование.

Контроль выполнения мероприятий по мере их выполнения должен осуществляться лицами, ответственными за безопасность СБЗС-систем на соответствующих стадиях жизненного цикла систем.

6.4 Все лица, ответственные за действия по управлению функциональной безопасностью, должны быть информированы о возложенной на них ответственности.

6.5 Поставщики оборудования и услуг для организации, ответственной за одну и более стадий полного жизненного цикла E/E/PE СБЗС-системы, ее аппаратных средств или программного обеспечения (см. 6.2), должны поставлять оборудование и оказывать услуги в соответствии с требованиями этой организации и должны иметь соответствующую систему менеджмента качества.

Примечание — Базовые требования к системам менеджмента качества установлены в стандартах ГОСТ Р ИСО 9000 и ГОСТ Р ИСО 9001.

7 Требования к полному жизненному циклу систем

7.1 Общие положения

7.1.1 Базовая техническая структура полного жизненного цикла СБЗС-систем и жизненного цикла зданий и сооружений, охватывающая основные действия, необходимые для достижения и поддержания требуемой полноты функциональной безопасности E/E/PE СБЗС-систем показана на рисунке 1.

Структура полного жизненного E/E/PE СБЗС-систем конкретного объекта может быть дополнена, сокращена или изменена при условии обоснования новой структуры и обеспечения выполнения целей и требований настоящего стандарта.

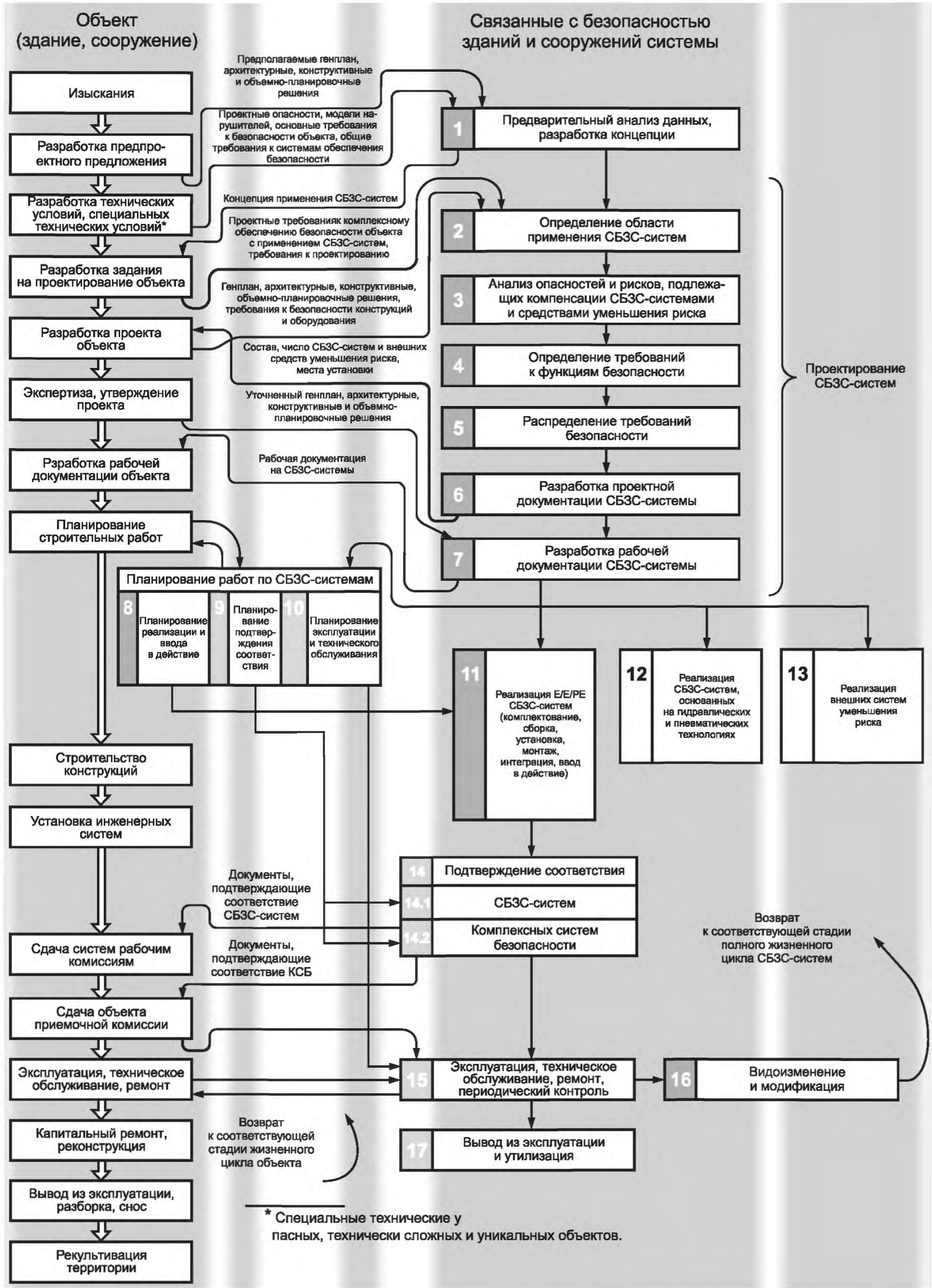


Рисунок 1 — Базовая структура полного жизненного цикла E/E/PE СБЗС-систем и жизненного цикла зданий и сооружений

В течение одного жизненного цикла объекта (здания или сооружения) может пройти несколько жизненных циклов E/E/PE СБЗС-систем.

Действия, относящиеся к верификации, управлению и оценке функциональной безопасности, не показанные на рисунке, относятся ко всем стадиям жизненного цикла E/E/PE СБЗС-систем, жизненных циклов аппаратных средств и программного обеспечения. Они должны быть выполнены, и результаты действий — документированы.

7.1.2 Для каждой конкретной E/E/PE СБЗС-системы должны быть установлены в документации, создаваемой на разных стадиях жизненного цикла, и выполнены все необходимые итеративные действия, относящиеся к определенным стадиям или существующие между стадиями, не отображенные на рисунке 2, в том числе действия, относящиеся:

- к верификации в соответствии с 7.19;
- к оценке функциональной безопасности в соответствии с разделом 8.

7.1.3 При проектировании должно быть проведено структурирование стадий в полном жизненном цикле E/E/PE СБЗС-систем, в которых должны быть установлены соответствующие действия для достижения требуемой функциональной безопасности.

7.1.4 Детальное структурирование стадий жизненного цикла аппаратных средств и программного обеспечения E/E/PE СБЗС-систем с требованиями к ним может быть установлено в стандартах на СБЗС-системы и СБЗС ПО.

7.1.5 Информация, относящаяся к функциональной безопасности E/E/PE СБЗС-систем, должна быть документирована на протяжении всего жизненного цикла систем.

7.1.6 Требования к управлению функциональной безопасностью, в соответствии с разделом 6, должны выполняться параллельно со стадиями полного жизненного цикла E/E/PE СБЗС-систем. Должна быть применена каждая стадия полного жизненного цикла E/E/PE СБЗС-систем, и должны быть выполнены все соответствующие требования.

7.1.7 Каждая стадия полного жизненного цикла E/E/PE СБЗС-системы должна быть разделена на элементарные действия с указанием для каждой стадии области определения, ее входных данных — входов и результатов — выходов.

7.1.8 Результаты (выходы) каждой стадии полного жизненного цикла E/E/PE СБЗС-систем должны удовлетворять целям и требованиям, заданным для каждой стадии в 7.2 — 7.18.

7.1.9 Для каждой стадии жизненного цикла E/E/PE СБЗС-систем должны быть выполнены требования к верификации, установленные в 7.19.

7.2 Разработка концепции (см. блок 1 на рисунке 1)

7.2.1 На стадии разработки концепции СБЗС-систем должны быть рассмотрены и учтены:

- предусмотренные предпроектными предложениями (при их наличии) характеристики здания и сооружения, предварительные генеральный план, объемно-планировочные и конструктивные решения, инженерные системы и управляемое оборудование, предполагаемые для применения в конкретном здании и сооружении, их функции управления и физическое окружение;
- информация о вероятных источниках опасности природного, техногенного и антропогенного характера, опасных воздействиях, моделях нарушителей, с учетом местных условий.
- требования действующих технических регламентов, национальных стандартов и сводов правил по безопасности зданий и сооружений, общие требования к объемно-планировочным решениям (в случае применения СБЗС-систем), низковольтному оборудованию.
- опасности, вызванные взаимодействием каждого управляемого оборудования (УО) с другими УО, установленными или планируемыми к установке вблизи рассматриваемого УО.

7.2.2 Информация и требования, установленные в 7.2.1, должны быть проанализированы и документированы; они должны быть учтены лицами, ответственными за разработку задания на проектирование объекта.

7.3 Определение области применения (см. блок 2 на рисунке 1)

7.3.1 В целях задания диапазона проектных техногенных, природных, антропогенных опасностей, установленных техническими условиями (специальными техническими условиями) и/или заданием на проектирование, подлежащих компенсации E/E/PE СБЗС-системами, а также дальнейшего определения необходимых функций безопасности, в зависимости от окружения УО, систем управления УО, особенностей объекта, его окружения и факторов риска, должны быть определены:

- конкретное оборудование, включая УО и системы управления УО,
- объемно-планировочные, конструктивные и инженерные решения, которые следует учитывать при анализе опасностей и риска,

- влияние внешних и внутренних событий и проектных моделей угроз, которые должны быть учтены при анализе опасностей и риска,

- системы и подсистемы, связанные с опасностями и риском,

- типы требующих анализа событий, приводящих к аварии, несчастному случаю, катастрофе (например, отказы компонентов, процедур, ошибки человека, зависимые механизмы отказов, нарушение прочности, устойчивости и иные факторы, которые могут привести к последовательности опасных событий),

- виды опасностей и факторы риска, приведенные в разделе 6 и приложениях Б и В ГОСТ Р 53195.1.

7.3.2 Результаты, полученные в 7.3.1, должны быть документированы.

7.4 Анализ опасностей и риска (см. блок 3 на рисунке 1)

7.4.1 При анализе опасностей и риска должны быть учтены установленные техническими условиями (специальными техническими условиями) и/или заданием на проектирование требования, представленные разработчиком(ами) соответствующих разделов проекта объекта, архитектурные, конструктивные, инженерные решения и уровень остаточного риска, обусловленного этими решениями, с учетом рисков примененного оборудования инженерных систем.

7.4.2 Должны быть определены:

- последовательности событий, приводящих к опасным событиям;

- опасности и опасные ситуации для УО и систем управления УО во всех режимах работы (штатных, предаварийных, аварийных) для обоснованных случаев, включая условия появления отказов и предсказуемого неправильного применения аппаратных средств и программного обеспечения E/E/PE СБЗС-систем;

- риски УО, связанные с опасными событиями.

7.4.3 Должен быть проведен анализ опасностей и риска, который учитывает результаты, полученные в 7.3.1, 7.4.1, 7.4.2. При этом может потребоваться проведение нескольких вариаций анализа опасностей и риска с различными возможными последовательностями развития опасных событий. Число вариаций анализа определяется проектировщиком СБЗС-систем.

7.4.4 При анализе особое внимание должно быть уделено нештатным или редко случающимся режимам работы УО.

7.4.5 Должен быть проведен анализ возможности предотвращения опасного события или последовательности опасных событий путем изменения архитектурных, объемно-планировочных, конструктивных и инженерных решений, модификации процесса разработки E/E/PE СБЗС-систем, модификации аппаратных средств и программного обеспечения.

7.4.6 Должны быть определены возможные последствия опасных событий и оценена вероятность их возникновения для условий, определенных в 7.4.3. Вероятность конкретного события может быть выражена количественно или качественно.

7.4.7 Для каждого конкретного опасного события должен быть вычислен или оценен риск УО.

7.4.8 Для выполнения требований 7.4.1 — 7.4.7 могут быть применены методы количественного или качественного анализа опасностей и риска, приведенные в приложениях Е — И ГОСТ Р 53195.1.

7.4.9 Для определения пригодности методов и возможности их применения следует учитывать факторы, включая:

- конкретные опасности и последствия;

- технические достижения в области строительства и безопасности, проверенные на практике;

- требования норм правового и технического регулирования в области строительства и безопасности;

- риск УО;

- наличие точных данных, на основании которых проводится анализ опасностей и рисков.

7.4.10 При анализе опасностей и рисков должны быть учтены:

- каждое установленное опасное событие и компоненты E/E/PE СБЗС-систем, которые ему способствуют;

- последствия и вероятность наступления события, с которым связано опасное событие;

- необходимое снижение риска для каждого опасного события;

- меры, принятые для снижения или предотвращения опасностей и риска;

- допущения, сделанные при анализе риска, включая оцененные или рассчитанные частоты запросов и частоты или интенсивность отказов оборудования; при этом должно быть детализировано любое действие, принятое для эксплуатационных ограничений, или вмешательство человека;

- документированная информация (см. раздел 5 и приложение А), относящаяся к E/E/PE СБЗС-системам на предыдущих стадиях их жизненного цикла, включая действия по верификации и подтверждению соответствия.

7.4.11 Информация и результаты анализа опасностей и рисков должны быть документированы и сохранены вплоть до вывода E/E/PE СБЗС-систем из эксплуатации и утилизации.

7.5 Определение требований к функциям безопасности (см. блок 4 на рисунке 1)

7.5.1 Перечень требований безопасности должен быть расширен при использовании СБЗС-систем, основанных на гидравлических и пневматических технологиях, и внешних средств уменьшения риска.

В случаях, когда могут быть сделаны обоснованные допущения о рисках, вероятности опасностей, опасных событиях и их последствиях, и имеются результаты анализа, предусмотренного в 7.4, требования могут быть представлены в упрощенной графической форме, в соответствии с ГОСТ Р 53195.1, приложения Ж и И.

Примечание — Настоящий стандарт не содержит требований к СБЗС-системам, основанным на гидравлических и пневматических технологиях. В случае применения таких систем в стандарте учитывается лишь обеспечиваемое ими снижение уровня риска.

7.5.2 Для каждой проектной опасности должны быть определены функции безопасности, реализуемые СБЗС-системами и внешними средствами уменьшения риска, необходимые для обеспечения требуемой безопасности зданий и сооружений. Должна быть определена спецификация требований к функциям безопасности и к полноте безопасности.

7.5.3 Для каждого заданного опасного события количественным и/или качественным методом должно быть определено необходимое снижение риска.

7.5.4 В случаях, когда отказы системы управления УО вызывают запросы к одной или нескольким СБЗС-системам и когда система управления УО не назначена как связанная с безопасностью система, должны выполняться следующие требования:

а) частота или интенсивность опасных отказов, требующаяся для системы управления УО, должна быть подкреплена данными, полученными:

- на основании практического опыта работы системы управления УО в аналогичном применении или
- на основе достоверного анализа, осуществленного по официально признанной процедуре (например, установленной в национальных стандартах, сводах правил), либо
- из промышленной базы данных по надежности оборудования этого вида;

б) частота или интенсивность опасных отказов, которая может потребоваться для систем управления УО, должна быть не ниже, чем 10^{-5} опасных отказов в час;

в) при разработке перечня полных требований безопасности должны быть определены и приняты во внимание все обоснованно предсказуемые режимы опасных отказов системы управления УО;

г) система управления УО должна быть отделена и независима от других СБЗС-систем и внешних средств снижения риска.

7.5.5 Если требования 7.5.4 не могут быть выполнены, то система управления УО должна рассматриваться как система, связанная с безопасностью. Уровень ее полноты безопасности должен быть выражен в величинах отказов по запросам в соответствии с пределами целевых отказов, установленными в 7.6.9 и 7.6.10. В этом случае требования настоящего стандарта, относящиеся к E/E/PE СБЗС-системам, должны быть применены к системам управления УО.

Примечание — Например, если для системы управления УО заявлена частота отказов в интервале 10^{-6} — 10^{-5} отказов в час, то требования, соответствующие уровню полноты безопасности SIL1, не должны выполняться.

7.5.6 Для каждой функции безопасности должно быть определено требование к полноте безопасности как требование необходимого снижения риска. Оно должно быть включено в полную спецификацию требований к полноте безопасности.

7.5.7 Полная спецификация требований к функции безопасности должна включать в себя перечень требований к функции безопасности — ее назначению (см. 7.5.2) — и перечень требований к полноте безопасности (см. 7.5.6).

7.6 Распределение требований безопасности (см. блок 5 на рисунке 1)

7.6.1 Функции безопасности, содержащиеся в полной спецификации требований безопасности (требований к функциям безопасности и требований к полноте безопасности) и уровни полноты безопасности для каждой функции безопасности должны быть распределены по назначенным E/E/PE СБЗС-системам, СБЗС-системам, основанным на других технологиях, и внешним средствам уменьшения риска.

При распределении требование к полноте безопасности в соответствии с 7.5 следует определять как требование необходимого снижения риска.

Примечания

1 Настоящий пункт применяется только тогда, когда хотя бы одна из СБЗС-систем является E/E/PE-системой.

2 СБЗС-системы, основанные на других технологиях, и внешние средства уменьшения риска, принимают во внимание только тогда, когда распределение по связанным с безопасностью E/E/PE-системам не приводит к необходимому снижению риска иначе, как с использованием этих систем и средств.

3 Требования к СБЗС-системам, основанным на других технологиях, и к стадиям их жизненного цикла не определяются настоящим стандартом. Стандартом учитывается лишь уровень снижения риска этими системами в случае их использования.

7.6.2 При распределении требований безопасности по назначенным СБЗС-системам и внешним средствам уменьшения риска проектировщиком должны быть приняты во внимание квалификация персонала и ресурсы, которые в период эксплуатации систем должны быть в распоряжении лиц, ответственных за их эксплуатацию.

7.6.3 Каждая функция безопасности с относящимся к ней требованием к полноте безопасности, расширенном в соответствии с 7.5, должна быть распределена по назначенным E/E/PE СБЗС-системам с учетом снижения риска, полученного с помощью СБЗС-систем, основанных на других технологиях, и внешних средств уменьшения риска (рисунок 2), таким образом, чтобы для этой функции безопасности было достигнуто необходимое снижение риска.

Если обнаруживается, что необходимое снижение риска не может быть достигнуто, то структура системы должна быть изменена, и распределение требований безопасности по системам и средствам должно быть проведено вновь.

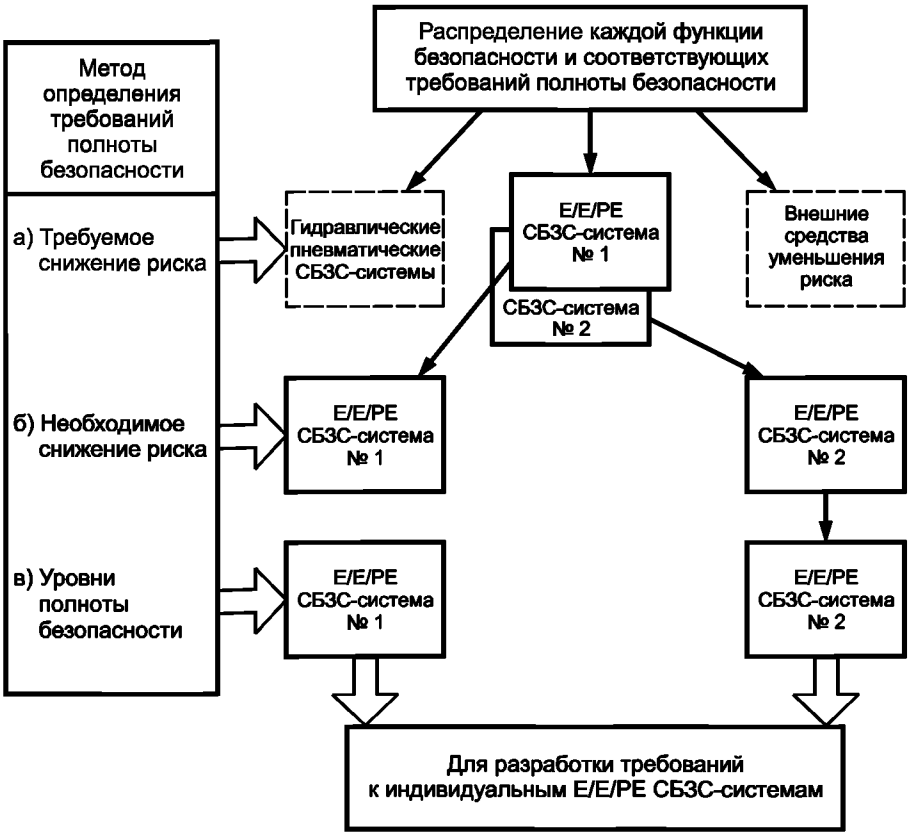


Рисунок 2 — Распределение требований безопасности по СБЗС-системам и внешним средствам уменьшения риска

7.6.4 Распределение функций и требований безопасности по системам и средствам уменьшения риска, указанное в 7.6.3, должно быть выполнено таким образом, чтобы все функции безопасности были распределены, и для каждой функции безопасности были выполнены требования к полноте безопасности.

7.6.5 Требования к полноте безопасности для каждой функции безопасности должны быть представлены таким образом, что каждая целевая величина полноты безопасности являлась:

- средней вероятностью отказов от выполнения ее назначенной функции по запросу (для режима работы с низкой частотой запросов) или

- вероятностью опасного отказа в час (для режима работы с высокой частотой запросов или с непрерывными запросами).

7.6.6 Распределение требований к полноте безопасности должно осуществляться с использованием комбинации вероятностей, с применением количественных или качественных методов.

7.6.7 В ходе распределения функций безопасности должна учитываться вероятность отказов с общей причиной.

7.6.8 Чтобы СБЗС-системы и внешние средства уменьшения риска при распределении могли рассматриваться как независимые системы и средства, они должны:

- быть функционально различными, т. е. использующими различные подходы для получения одних и тех же результатов;

- основываться на различных технологиях, т. е. в них должны быть использованы различные принципы действия и/или виды оборудования для получения одних и тех же результатов;

- не содержать общих частей, систем сервиса или поддержки, например, источников питания, отказ которых может привести в опасном режиме к отказу всех систем;

- не использовать общих процедур эксплуатации, технического обслуживания и тестирования;

- быть физически разделенными таким образом, чтобы предсказуемые отказы не влияли на избыточные СБЗС-системы и внешние средства уменьшения риска.

7.6.9 Если не все требования 7.6.8 могут быть выполнены, то СБЗС-системы и внешние средства уменьшения риска при распределения полноты безопасности не могут считаться независимыми до тех пор, пока в результате проведенного анализа не будет доказано, что они полностью независимы с точки зрения полноты безопасности.

7.6.10 На завершающем этапе распределения требований к полноте безопасности для каждой функции безопасности, распределенной по E/E/PE СБЗС-системам, требования должны быть выражены в значениях целевых величин отказов в зависимости от уровней полноты безопасности в соответствии с таблицами 1 и 2.

Таблица 1 — Целевая величина отказов по запросам для функции безопасности, действующей в режиме работы с низкой частотой запросов L

Уровень полноты безопасности	Значение целевой величины отказов функции безопасности (средней вероятности опасных отказов по запросам от выполнения назначенной функции)
SIL 4	От 10^{-5} включ. до 10^{-4}
SIL 3	От 10^{-4} включ. до 10^{-3}
SIL 2	От 10^{-3} включ. до 10^{-2}
SIL 1	От 10^{-2} включ. до 10^{-1}

Таблица 2 — Целевая величина отказов по запросам для функции безопасности, действующей в режиме работы с высокой частотой запросов H или с непрерывным запросом

Уровень полноты безопасности	Значение целевой величины отказов функции безопасности (вероятности опасных отказов в час)
SIL 4	От 10^{-9} включ. до 10^{-8}
SIL 3	От 10^{-8} включ. до 10^{-7}
SIL 2	От 10^{-7} включ. до 10^{-6}
SIL 1	От 10^{-6} включ. до 10^{-5}

Величины полноты безопасности должны быть представлены как

- средняя вероятность отказов при выполнении ее назначенной функции по запросу (для режима работы с низкой частотой запросов) или

- вероятность опасных отказов в час (для режима работы с высокой частотой запросов или с постоянным запросом).

7.6.11 Для E/E/PE СБЗС-систем, работающих в режиме с высокой частотой запросов или с постоянным запросом, для которых во время выполнения задания восстановление невозможно, требуемый уровень полноты безопасности может быть получен следующим образом. Вначале определяют требуемую вероятность отказов при выполнении функции безопасности в течение времени выполнения задания и делят ее на время выполнения задания для получения требуемой вероятности отказов в час. Затем используют таблицу 2 для получения требуемого уровня полноты безопасности.

7.6.12 Для E/E/PE СБЗС-системы, которая выполняет функции безопасности различного уровня полноты безопасности, те части аппаратных средств и программного обеспечения, которые недостаточно независимы при реализации функций безопасности, должны рассматриваться как выполняющие функции безопасности с наивысшим уровнем полноты безопасности. До тех пор, пока на основании анализа не будет доказана достаточная независимость этих индивидуальных функций безопасности, на эти части должны быть распространены требования, применимые к наивысшему значимому уровню полноты безопасности.

7.6.13 Структура СБЗС-системы, состоящая из одиночной E/E/PE-системы с уровнем полноты безопасности SIL 4, может быть допущена к применению только в случае, если будет выполняться перечисление а), либо одновременно оба перечисления б) и в), приведенные ниже:

а) значение величины отказов при выполнении функций безопасности для целевой полноты безопасности получено с использованием комбинации соответствующих аналитических методов и тестирования;

б) имеется обширный опыт эксплуатации компонентов, используемых как часть E/E/PE СБЗС-системы, полученный в условиях подобной окружающей среды и в системе сопоставимого уровня сложности;

в) имеются достоверные данные по отказам аппаратуры, состоящей из компонентов, используемых как часть E/E/PE СБЗС-системы, соответствующие требуемым целевым значениям полноты безопасности. Указанные данные по отказам должны относиться к планируемой окружающей среде, применению и сложности.

7.6.14 Ни одна одиночная связанная с безопасностью E/E/PE СБЗС-система не должна быть размещена по целевой величине отказов для требуемой полноты безопасности ниже, чем указано в таблицах 1 и 2. То есть, для E/E/PE СБЗС-систем, работающих в режиме с низкой частотой запросов для обеспечения ее назначенной функции по запросу, нижний предел должен быть установлен как средняя вероятность опасных отказов 10^{-5}, а для систем, работающих в режиме с высокой частотой запросов или с постоянным запросом, нижний предел должен быть установлен как вероятность 10^{-9} опасных отказов в час.

7.6.15 Информация и результаты распределения требований безопасности, полученные в 7.6.2 — 7.6.14, а также все сделанные допущения и обоснования должны быть документированы.

7.7 Разработка проектной документации на СБЗС-системы (см. блок 6 на рисунке 1)

7.7.1 В проектной документации на здания и сооружения должен быть предусмотрен раздел «Мероприятия по комплексному обеспечению безопасности» для обеспечения дальнейших действий по реализации жизненного цикла СБЗС-систем и жизненного цикла зданий и сооружений.

7.7.2 Разработка проектной документации на СБЗС-системы должна осуществляться лицами с уровнем компетентности, достаточным для выполнения проектных работ по созданию систем безопасности зданий и сооружений данной категории сложности и ответственности.

7.7.3 Разработка проектной документации на СБЗС-системы должна осуществляться в соответствии с процедурами, предусмотренными принятой в проектной организации системой менеджмента качества, не противоречащей требованиям ГОСТ Р ИСО 9001.

7.7.4 Проектная документация должна содержать:

- перечень и состав всех СБЗС-систем и внешних средств уменьшения риска, предусмотренных 7.6, включая наименование и версию программного обеспечения, используемого для каждой из E/E/PE СБЗС-систем или подсистем;

- структурную и/или функциональную схему каждой из E/E/PE СБЗС-систем, схемы соединений их составляющих, схемы соединения с УО или системами управления УО, схемы соединений с источниками питания;

- структурную и/или функциональную схему комплексной системы безопасности;

- схемы соединений СБЗС-систем при объединении их в комплексную систему безопасности;

- структурную схему главного центра управления (центра управления кризисными ситуациями), а также структурные схемы периферийных центров управления и резервного пункта управления службы безопасности зданий и сооружений (при их наличии);

- наименование и краткое описание прикладного программного обеспечения, применяемого для интеграции программируемых электронных СБЗС-систем в систему комплексной безопасности зданий и сооружений, включая описание способов достижения информационной совместимости систем;

- структурные и/или функциональные схемы взаимодействия с оборудованием внешних служб (МЧС, экстренной медицинской помощи, МВД, ФСБ, внешних диспетчерских служб) и внутренних диспетчерских служб, а также схемы соединений с этим оборудованием;

- описание алгоритмов взаимодействия СБЗС-систем и подсистем в составе комплексной системы безопасности объекта:

- при нормальной эксплуатации в штатных режимах,

- в период проведения регламентных работ,

- в предаварийных ситуациях,

- при аварийных, кризисных и чрезвычайных ситуациях,

- в период ликвидации последствий чрезвычайных ситуаций;

- описание алгоритмов взаимодействия систем в период управления эвакуацией людей для нескольких (не менее трех) сюжетов развития опасных событий;

- описание алгоритмов взаимодействия службы безопасности объекта с внешними службами (МЧС, экстренной медицинской помощи, МВД, ФСБ, внешними диспетчерскими службами) и внутренними диспетчерскими службами;

- требования к размещению оборудования и периферийных средств контроля и управления E/E/PE СБЗС-систем; при этом особое внимание должно быть уделено:

- контролю жизненно важных помещений, зон и критически важных точек объекта,

- контролю путей эвакуации людей,

- одновременному применению в ответственных зонах элементов контроля и управления различных E/E/PE СБЗС-систем для повышения их эффективности;

- состав и схемы размещения оборудования в центральном и резервном (при его наличии) пунктах управления службы безопасности объекта;

- требования к организации кабельных каналов;

- схемы прокладки кабельных трасс;

- требования к техническим средствам защиты информации;

- спецификация оборудования и материалов E/E/PE СБЗС-систем.

7.7.5 В случае применения СБЗС-систем, основанных на других технологиях, и внешних средств уменьшения риска, требования к ним и их характеристики должны быть включены в комплект проектной документации.

7.7.6 Документацию следует оформлять в соответствии с требованиями, изложенными в разделе 5 и рекомендациями приложения А.

7.7.7 По завершении разработки раздела проекта должен быть проведен аудит документации, перечисленной в 7.7.2 — 7.7.5, с привлечением независимого эксперта (экспертов), независимого подразделения или независимой организации.

7.7.8 Документация раздела «Мероприятия по комплексному обеспечению безопасности» проекта, указанного в 5.2.3, должна быть согласована с заинтересованными подразделениями и/или организациями (указанными в специальных технических условиях и/или задании на проектирование) и утверждена в установленном порядке.

7.7.9 После утверждения документация раздела проекта по 5.2.3 должна быть доступна лицам, ответственным за разработку проекта на здания и сооружения.

7.7.10 Документация раздела проекта по 5.2.3, включая все последующие внесенные по установленным процедурам изменения и дополнения, должна быть сохранена в хронологическом порядке вплоть до полного завершения жизненного цикла СБЗС-систем, комплексной системы безопасности и объекта.

7.8 Разработка рабочей документации (см. блок 7 на рисунке 1)

7.8.1 Для обеспечения должного выполнения действий по реализации последующих стадий жизненного цикла E/E/PE СБЗС-систем и комплексной системы безопасности, а также жизненного цикла зданий и сооружений должна быть разработана рабочая документация на эти системы.

7.8.2 При разработке рабочей документации на E/E/PE СБЗС-системы и комплексную систему безопасности должны быть учтены архитектурные, объемно-планировочные, конструктивные и инженерные решения утвержденного в установленном порядке проекта на здания и сооружения.

7.8.3 В комплект рабочей документации на СБЗС-системы и комплексную систему безопасности должны входить как минимум следующие документы:

а) рабочие чертежи главного центра управления службы безопасности зданий и сооружений (центра управления кризисными ситуациями), периферийных центров и резервного пункта управления (при их наличии);

б) рабочие чертежи на монтаж оборудования и периферийных устройств СБЗС-систем;

в) рабочие чертежи (строительные задания) на прокладку кабелей E/E/PE СБЗС-систем;

г) кабельные журналы;

д) инструкции по установке (монтажу), пуску, регулированию оборудования и периферийных средств СБЗС-систем;

е) программное обеспечение для E/E/PE СБЗС-систем и руководства к ним;

ж) тестовые программы для контроля E/E/PE СБЗС-систем и руководства к ним;

и) базовые методы испытаний и оценки соответствия E/E/PE СБЗС-систем, их аппаратных средств и программного обеспечения;

к) руководства по эксплуатации СБЗС-систем;

л) инструкция по интеграции E/E/PE СБЗС-систем в систему комплексной безопасности, пуско-наладке системы;

м) тестовые программы для контроля комплексной системы безопасности и руководства к ним;

н) базовые методы испытаний и оценки соответствия комплексной системы безопасности, аппаратных средств и программного обеспечения;

п) руководство по эксплуатации комплексной системы безопасности;

р) формуляры (журналы) на СБЗС-системы;

с) формуляр на комплексную систему безопасности;

т) каталог СБЗС-систем и их составляющих;

у) нормы расхода запасных частей (если они предусмотрены);

ф) нормы расхода материалов (если они предусмотрены);

х) ведомость комплекта запасных частей, инструментов, принадлежностей и материалов (если они предусмотрены);

ц) эксплуатационные специальные инструкции, при необходимости.

7.8.4 Содержание и оформление эксплуатационных документов должно соответствовать требованиям ГОСТ 2.610.

7.8.5 До реализации и ввода в действие E/E/PE СБЗС-систем, подтверждения их соответствия настоящему стандарту, а также эксплуатации и технического обслуживания лицами, ответственными за выполнение работ на этих стадиях должны быть разработаны и согласованы с проектной организацией планы проведения этих работ.

7.9 Планирование полной установки, интеграции и ввода в действие (см. блок 8 на рисунке 1)

7.9.1 Для обеспечения достижения требуемой функциональной безопасности до установки оборудования СБЗС-систем в зданиях и сооружениях должны быть разработаны в контролируемой форме планы:

- реализации, установки (монтажа) E/E/PE СБЗС-систем;
- ввода в действие E/E/PE СБЗС-систем;
- интеграции E/E/PE СБЗС-систем в единую систему комплексной безопасности зданий и сооружений.

7.9.2 Лицами, ответственным за реализацию систем на объекте, должен быть разработан план установки (монтажа) E/E/PE СБЗС-систем, определяющий:

- график установки;
- лиц, ответственных за установку различных частей;
- процедуры по установке;
- последовательность, в которой интегрируются отдельные части;
- критерии для декларирования наличия всех частей E/E/PE СБЗС-систем для их установки и для декларирования завершения действий по установке;
- процедуры по устранению недостатков, повреждений, аварий и несовместимости.

7.9.3 План ввода в действие E/E/PE СБЗС-систем должен определять:

- график ввода в действие;

- лиц, ответственных за ввод в действие систем и их частей;
- процедуры по вводу в действие систем;
- взаимосвязи и взаимоотношения при выполнении отдельных действий по установке и вводу в действие систем;
- взаимосвязи и взаимоотношения при подтверждении соответствия систем техническим требованиям.

7.9.4 План интеграции E/E/PE СБЗС-систем в единую систему комплексной безопасности зданий и сооружений должен определять:
- график интегрирования систем;
- лиц, ответственных за интегрирование систем;
- взаимосвязи и взаимоотношения при осуществлении интегрирования систем;
- взаимосвязи и взаимоотношения при подтверждении соответствия системы комплексной безопасности техническим требованиям.

7.9.5 План полной установки, ввода в действие и интеграции E/E/PE СБЗС-систем в единую систему комплексной безопасности зданий и сооружений должен быть документирован.

7.10 Планирование подтверждения соответствия систем требованиям функциональной безопасности (см. блок 9 на рисунке 1)

7.10.1 Лицами, ответственными за реализацию СБЗС-систем в зданиях и сооружениях, должен быть разработан план подтверждения соответствия требованиям полной функциональной безопасности E/E/PE СБЗС-систем.

7.10.2 План должен предусматривать два этапа проведения подтверждения соответствия — подтверждение соответствия каждой из E/E/PE СБЗС-систем и подтверждение соответствия комплексной системы безопасности после интеграции E/E/PE СБЗС-систем в комплексную систему безопасности.

7.10.3 В случаях, предусмотренных проектной документацией на E/E/PE СБЗС-системы, допускается осуществлять оценку соответствия отдельных E/E/PE СБЗС-систем в составе комплексной системы безопасности после интеграции систем.

7.10.4 Оценка соответствия E/E/PE СБЗС-систем и комплексной системы безопасности зданий и сооружений должна осуществляться по методикам, разработанным на основе базовых методов в соответствии с 7.8.3, перечисления и) и н).

7.10.5 Разработанный план должен включать:
- порядок и график проведения подтверждения соответствия отдельных E/E/PE СБЗС-систем (до интеграции отдельных систем в комплексную систему безопасности согласно 7.10.2 или после интеграции отдельных систем в комплексную систему безопасности после интеграции систем в соответствии с 7.10.3) и комплексной системы безопасности;
- сведения о лицах, которые должны осуществлять подтверждение соответствия;
- перечень отдельных режимов работы УО во взаимодействии с E/E/PE СБЗС-системами, в том числе режимов работы:
- при подготовке систем к использованию, включая установку и настройку систем;
- при обучении и тренировке обслуживающего персонала;
- при пуске систем в автоматическом, ручном, полуавтоматическом режимах;
- в стационарном режиме;
- при переустановке;
- при отключении;
- при техническом обслуживании;
- при предсказуемом неправильном использовании оборудования систем;
- перечень E/E/PE СБЗС-систем, которые требуют подтверждения соответствия для каждого режима УО до начала ввода в действие;
- техническую стратегию для подтверждения соответствия, в том числе, методы анализа и методы испытаний;
- мероприятия, методы и процедуры, которые должны быть использованы для подтверждения правильности распределения функций безопасности, включая подтверждение, что каждая функция безопасности соответствует:
- перечню требований к полным функциям безопасности (аппаратных средств и ПО),
- перечню требований к полноте безопасности полных функций безопасности (аппаратных средств и ПО);
- индивидуальные ссылки на каждый элемент, использованный на выходах действий по 7.5 и 7.6;
- требования к окружающей среде при осуществлении действий по подтверждению соответствия;

- методику и процедуры для оценки результатов испытаний, расчетов, особенно отказов;
- критерии «соответствия»/«несоответствия» требованиям, а также возможности обхода систем.

7.10.6 При разработке плана подтверждения соответствия должны быть приняты во внимание результаты действий по планированию подтверждения функциональной безопасности аппаратных средств программируемых электронных систем и ПО; при этом следует удостовериться в том, что взаимовлияние между всеми принятыми мерами по снижению риска рассмотрено, и все действия, предусмотренные в 7.5, выполнены.

7.10.7 Для комплексных систем безопасности особо опасных, технически сложных и уникальных объектов в программу испытаний, являющихся частью действий по оценке соответствия, должны быть включены сюжеты (не менее трех), имитирующие неблагоприятное сочетание наиболее опасных событий в их развитии; при этом не менее двух сюжетов должны имитировать действия, осуществляемые при управлении эвакуацией людей из зданий и сооружений.

7.10.8 Информация по 7.10.2 — 7.10.7 должна быть документирована и сохранена.

7.11 Планирование эксплуатации и технического обслуживания систем (см. блок 10 на рисунке 1)

7.11.1 Лицами, ответственными за ввод в эксплуатацию зданий и сооружений, должен быть разработан план эксплуатации и технического обслуживания E/E/PE СБЗС-систем, в том числе комплексных систем безопасности, включая периодические контрольные проверки, для поддержания требуемой функциональной безопасности в период эксплуатации и технического обслуживания систем.

7.11.2 План должен содержать:

а) типовые действия, которые необходимо выполнять для поддержания требуемой функциональной безопасности E/E/PE СБЗС-систем, в том числе комплексных систем безопасности;

б) действия и ограничения, необходимые во время пуска в действие систем, при нормальной эксплуатации, стандартных испытаниях, предсказуемых нарушениях, отказах и отключениях для предупреждения опасного состояния, для снижения частоты запросов к E/E/PE СБЗС-системам, или снижения последствий опасных событий, в том числе:

- ограничения УО при эксплуатации во время неисправности или отказа E/E/PE СБЗС-систем;
- ограничения УО при эксплуатации в период технического обслуживания E/E/PE СБЗС-систем;
- действия, когда ограничения УО в период эксплуатации могут быть устранены;
- процедуры для возвращения к нормальной эксплуатации систем;
- процедуры, подтверждающие, что нормальная эксплуатация достигнута;
- ограничения, из-за которых функции E/E/PE СБЗС-системы могут быть не использованы для пуска, специального режима работы или тестирования;
- процедуры, которые должны следовать до, во время и после обхода E/E/PE СБЗС-систем, включая допуск к рабочим процедурам и уровни полномочий;

в) информацию о результатах аудита функциональной безопасности и тестирования, подлежащую сохранению;

г) информацию об опасных ситуациях и всех ситуациях, которые потенциально приводят к опасному событию, подлежащую сохранению;

д) масштаб действий по техническому обслуживанию, контрольным испытаниям и их периодичности;

е) действия, которые должны быть предприняты в случае появления опасных событий;

ж) перечень документации в хронологическом порядке по действиям в период эксплуатации и технического обслуживания (см. 7.16).

7.11.3 В плане должны быть указаны требования, предъявляемые к квалификации персонала, осуществляющего эксплуатацию E/E/PE СБЗС-систем и комплексной системы безопасности зданий и сооружений, а также квалификации персонала, осуществляющего техническое обслуживание этих систем.

7.11.4 Действия по техническому обслуживанию, которые осуществляются для обнаружения скрытых неисправностей, должны выполняться на основе систематического анализа.

7.11.5 План по техническому обслуживанию E/E/PE СБЗС-систем должен быть согласован с лицами, ответственными за будущую эксплуатацию и техническое обслуживание СБЗС-систем и внешних средств уменьшения риска, а также систем, не связанных с безопасностью, которые потенциально могут иметь запрос к СБЗС-системам.

7.12 Реализация E/E/PE СБЗС-систем (см. блок 11 на рисунке 1)

7.12.1 Реализация E/E/PE СБЗС-систем в зданиях и сооружениях должна предусматривать:

- подготовку E/E/PE-систем в соответствии с перечнем требований к E/E/PE СБЗС-системам, включая перечни требований к аппаратным средствам и программному обеспечению;

- установку (монтаж) систем на объекте;
- интеграцию E/E/PE СБЗС-систем в комплексную систему безопасности;
- ввод в действие систем в составе комплексной системы безопасности.

7.12.2 До установки (монтажа) аппаратных средств и программного обеспечения E/E/PE СБЗС-систем на объекте должно быть подтверждено их соответствие спецификации и требованиям безопасности, установленным в проектной документации.

7.12.3 Действия по установке (монтажу) должны выполняться в соответствии с документацией по установке (монтажу). Очередность и порядок выполнения работ должны соответствовать плану по установке (монтажу) E/E/PE СБЗС-систем.

7.12.4 Документация по установке (монтажу) E/E/PE СБЗС-систем должна включать:

- документацию по действиям по установке, регулировке и пуско-наладке E/E/PE СБЗС-систем и их составляющих;
- документацию по интегрированию систем в систему комплексной безопасности и вводу в действие;
- документацию по разрешению отказов и несовместимости.

7.13 Реализация СБЗС-систем, основанных на других технологиях (см. блок 12 на рисунке 1)

7.13.1 До установки СБЗС-систем, основанных на других (гидравлической и пневматической) технологиях, в зданиях и сооружениях должно быть подтверждено их соответствие спецификации и требованиям безопасности, установленным в проектной документации.

7.13.2 Перечень требований к функциональной безопасности и требований к полноте безопасности СБЗС-систем, основанных на других технологиях, не устанавливается настоящим стандартом.

7.14. Реализация внешних средств уменьшения риска (см. блок 13 на рисунке 1)

7.14.1 До реализации внешних средств уменьшения риска в зданиях и сооружениях и на прилегающих территориях должно быть подтверждено их соответствие требованиям безопасности, установленным в проектной документации.

7.14.2 Перечень требований к функциональной безопасности и требований к полноте безопасности внешних средств уменьшения риска не устанавливается настоящим стандартом.

7.15 Подтверждение соответствия (см. блок 14 на рисунке 1)

7.15.1 Лицами, ответственными за введение зданий и сооружений в эксплуатацию, должно быть организовано подтверждение соответствия установленных в них E/E/PE СБЗС-систем и комплексных систем безопасности полным требованиям функциональной безопасности к функциям безопасности и полноте безопасности (аппаратных средств и программного обеспечения), с учетом распределения безопасности по E/E/PE СБЗС-системам в соответствии с 7.6.

7.15.2 Действия по подтверждению соответствия должны осуществляться согласно плану подтверждения соответствия E/E/PE СБЗС-систем и комплексной системы безопасности предусмотренным требованиям (см. 7.10).

7.15.3 В документацию, составляемую в период подтверждения соответствия, должны быть включены:

- сведения о действиях по подтверждению соответствия, в хронологическом порядке;
- используемая версия спецификации полных требований к функциональной безопасности;
- перечень функций безопасности, соответствие которых подтверждается с помощью испытаний или анализа;
- перечень средств испытаний, измерительных приборов и данные об их аттестации и поверке;
- результаты действий по подтверждению соответствия;
- подробная идентификация пункта испытаний, применяемых процедур и условий испытаний;
- сведения о различии между ожидаемыми и полученными фактическими результатами.

7.15.4 В случае расхождений между ожидаемыми и фактическими результатами должны быть документированы проведенный анализ и решение, принятое по продолжению подтверждения соответствия, либо решение по изменению порядка испытаний или анализа и возврата к более раннему этапу подтверждения соответствия.

7.16 Эксплуатация, техническое обслуживание, ремонт, периодический контроль (см. блок 15 на рисунке 1)

7.16.1 Эксплуатация, техническое обслуживание, ремонт и периодический контроль E/E/PE СБЗС-систем и комплексной системы безопасности должны осуществляться таким образом, чтобы в период эксплуатации систем поддерживались заданные требования функциональной безопасности.

7.16.2 Должно обеспечиваться выполнение:

- плана эксплуатации и технического обслуживания E/E/PE СБЗС-систем, комплексной системы безопасности (см. 7.11);

- процедур эксплуатации и технического обслуживания E/E/PE СБЗС-систем;
- процедур эксплуатации и поддержки программного обеспечения E/E/PE СБЗС-систем;
- процедур периодических проверок (испытаний) E/E/PE СБЗС-систем и комплексной системы безопасности, в том числе органами государственного контроля (надзора).

7.16.3 Выполнение положений, приведенных в 7.16.2, должно включать в себя:
- следование графику технического обслуживания;
- исполнение процедур;
- ведение документации;
- периодическое осуществление аудита (проверки) функциональной безопасности;
- документирование сделанных модификаций E/E/PE СБЗС-систем.

Пример модели действий в период эксплуатации и технического обслуживания показан на рисунке 3. Пример модели управления эксплуатацией и техническим обслуживанием показан на рисунке 4.

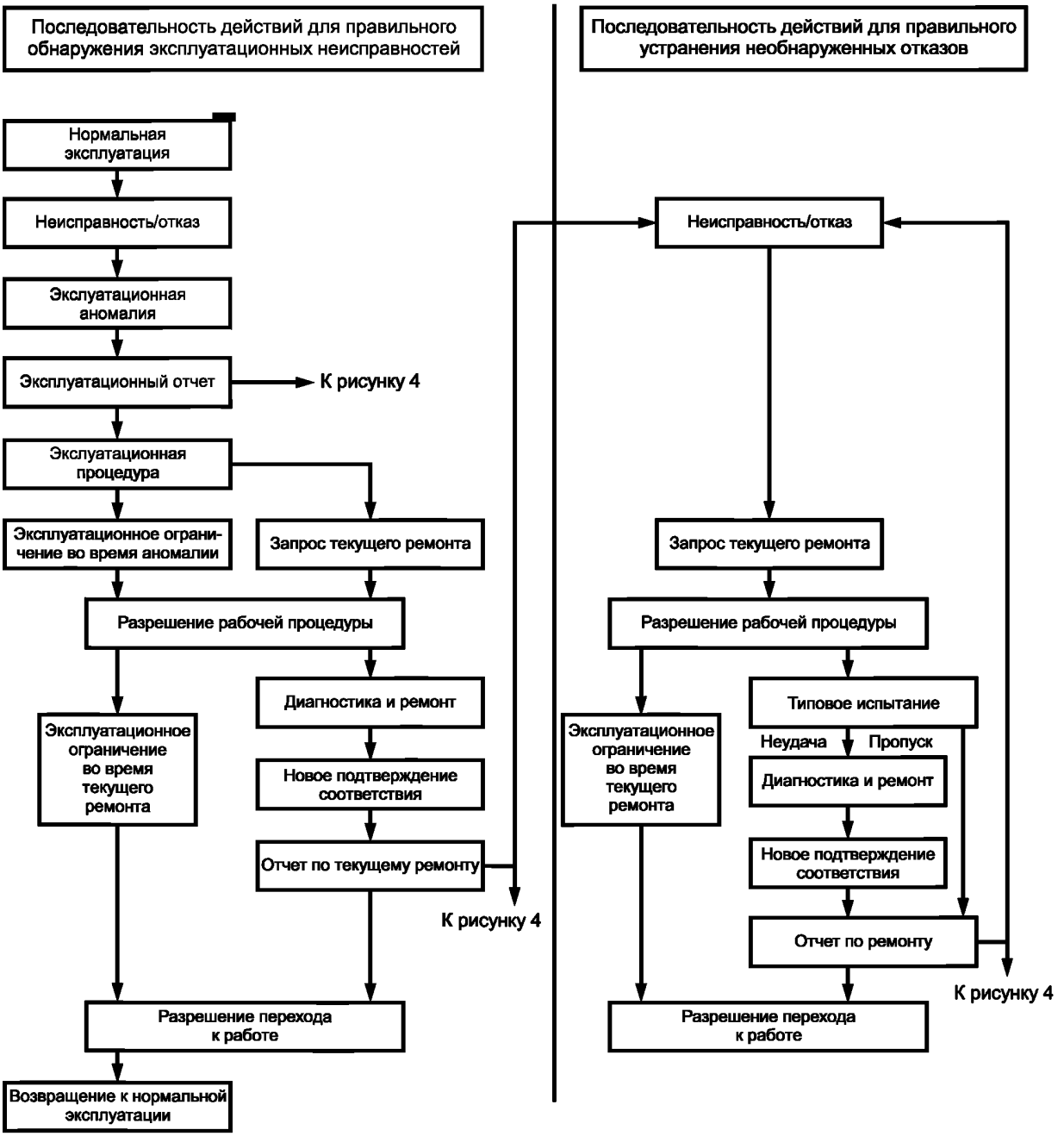


Рисунок 3 — Пример модели эксплуатации и текущего ремонта

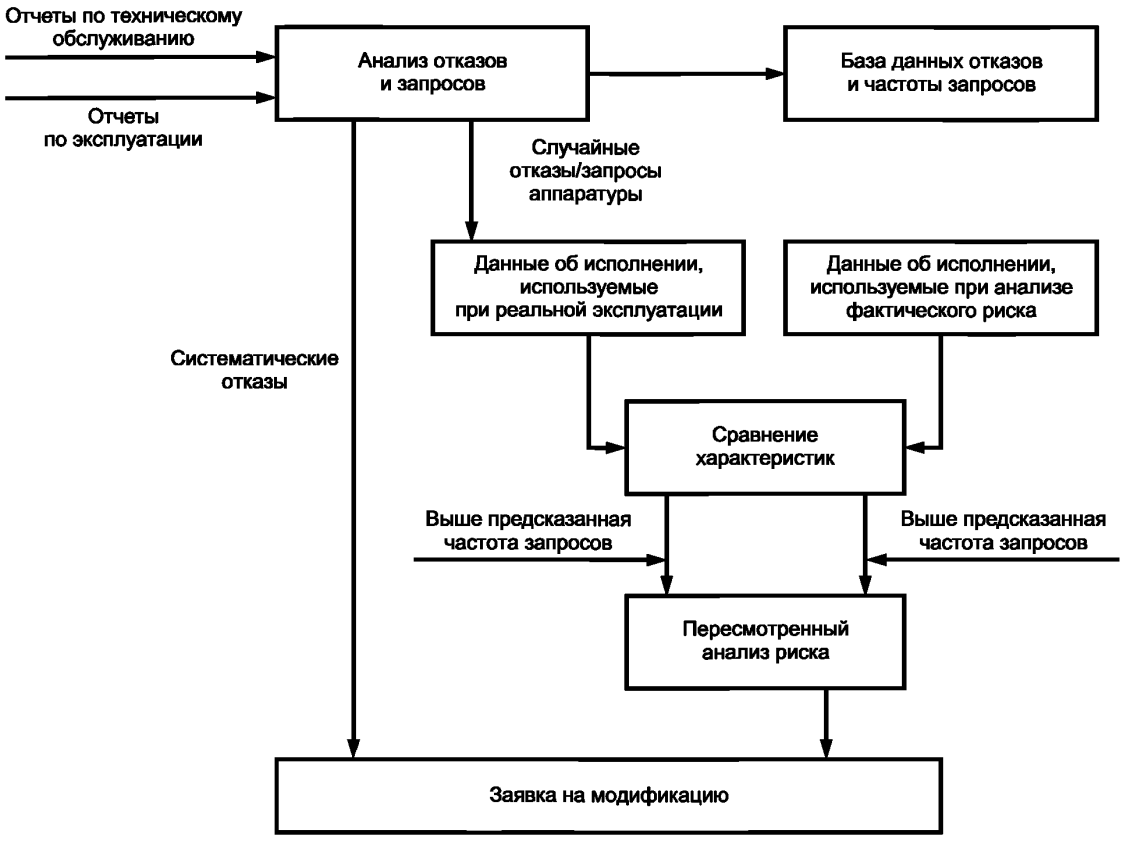


Рисунок 4 — Пример модели управления эксплуатацией и техническим обслуживанием

7.16.4 Документация, создаваемая в хронологическом порядке при эксплуатации, ремонте и техническом обслуживании E/E/PE СБЗС-систем, должна содержать:

- результаты аудита и испытаний (или тестирования) функциональной безопасности, в том числе органами государственного контроля (надзора);
- данные о времени и случаях запросов к E/E/PE СБЗС-системам в реальной эксплуатации и данные о поведении E/E/PE СБЗС-систем, когда эти запросы и отказы происходят в период профилактического технического обслуживания;
- данные о проведенных модификациях УО, систем управления УО и E/E/PE СБЗС-систем.

7.16.5 Документация должна сохраняться в течение всего периода эксплуатации систем, вплоть до вывода их из эксплуатации и утилизации.

7.17 Видоизменение и модификация (см. блок 16 на рисунке 1)

7.17.1 Видоизменение и модификация E/E/PE СБЗС-систем и комплексной системы безопасности должны осуществляться таким образом, чтобы требования функциональной безопасности обеспечивались как во время проведения видоизменения или модификации, так и после их завершения.

7.17.2 Перед проведением любого видоизменения и модификации E/E/PE СБЗС-систем и комплексной системы безопасности эти процедуры должны быть запланированы в соответствии с 6.2. Пример модели процедуры видоизменения и модификации показан на рисунке 5.

7.17.3 Стадия видоизменения или модификации может быть инициирована только на основании авторизованной заявки, оформленной в соответствии с процедурами управления функциональной безопасностью, указанными в разделе 6. Заявка должна содержать:

- заданные проектные опасности, которые могут иметь место;
- предлагаемые изменения аппаратных средств и/или программного обеспечения;
- обоснование для изменений.

Основанием для заявки на видоизменение и модификацию могут быть:

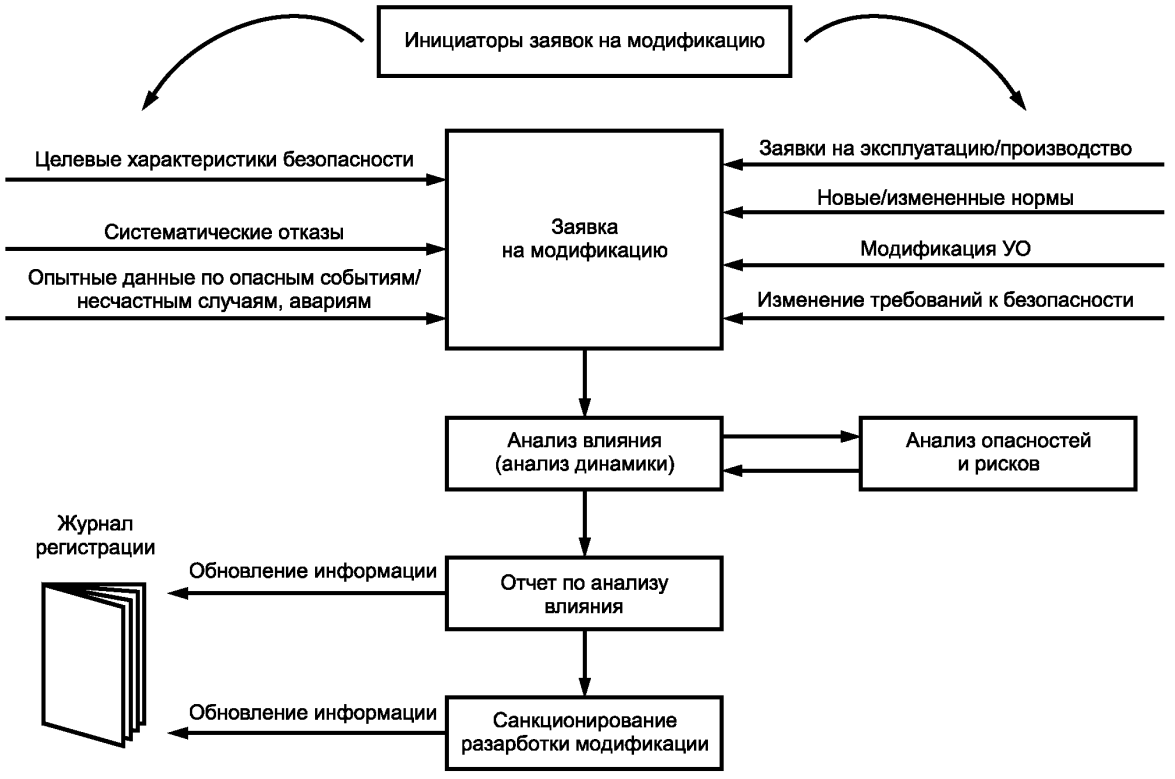


Рисунок 5 — Пример модели процедуры видоизменения и модификации

- подтвержденные сведения об отличии реальной функциональной безопасности от заданной функциональной безопасности;
- систематические отказы, обнаруженные при эксплуатации;
- новые или измененные нормы технического регулирования;
- модификации УО и условий их применений;
- результаты анализа эксплуатационных характеристик и характеристик технического обслуживания, указывающие, что фактические характеристики хуже планируемых характеристик;
- результаты регулярной проверки (аудита) функциональной безопасности;
- результаты проверки органами государственного контроля (надзора), установившие несоответствие требованиям безопасности, и соответствующее предписание органов контроля (надзора) по его устранению.

7.17.4 До осуществления видоизменения или модификации E/E/PE СБЗС-систем и комплексной системы безопасности должен проводиться анализ влияния, включающий в себя оценку влияния предложенного видоизменения и модификации либо действий по видоизменению или модификации на функциональную безопасность E/E/PE СБЗС-систем и комплексной системы безопасности.

7.17.5 Оценка влияния должна включать в себя анализ опасностей и рисков, которые могут возникнуть на последующих стадиях жизненного цикла E/E/PE СБЗС-систем и комплексной системы безопасности, их аппаратных средств или программного обеспечения. При оценке влияния должно также учитываться влияние других конкурирующих изменений и модификаций или действий по изменениям и модификациям и должна учитываться функциональная безопасность, имеющая место как в период осуществления видоизменений или модификаций, так и после проведения видоизменений и модификаций или действий по видоизменениям или модификациям.

7.17.6 Результаты, описанные в 7.17.5, должны быть документированы.

7.17.7 Разрешение на осуществление требуемого видоизменения или модификации, либо действий по видоизменению и модификации должно определяться с учетом результатов анализа влияния.

7.17.8 Все видоизменения и модификации, которые оказывают влияние на функциональную безопасность любой E/E/PE СБЗС-системы комплексной системы безопасности, должны начинаться с возврата к соответствующей стадии жизненного цикла системы, жизненного цикла аппаратных средств или программного обеспечения. Все последующие стадии должны быть осуществлены в соответствии с процедурами, установленными для соответствующих стадий, и требованиями настоящего стандарта.

7.17.9 В случае отличия реальных оцененных или измеренных уровней полноты безопасности от заданных для E/E/PE СБЗС-систем уровней полноты безопасности следует провести полный анализ опасностей и рисков.

7.17.10 Не допускается применение процедур тестирования, разработанных для начальной установки и пуска в действие E/E/PE СБЗС-систем, для работы с УО в режиме внешнего управления без проверки подтверждения соответствия систем и подтверждения практической целесообразности применения этих процедур.

7.17.11 Должна быть создана и сохранена в хронологическом порядке документация, содержащая детали всех видоизменений и модификаций. В указанную документацию должны быть включены ссылки на документы, содержащие:

- заявки на изменение и модификацию;
- результаты анализа влияния;
- результаты перепроверки (повторной верификации) и повторного подтверждения соответствия данным и результатам;

Также должны быть сохранены все документы, отражающие изменения и модификации, и действия по изменениям и модификациям.

7.18 Вывод из эксплуатации и утилизация (см. блок 17 на рисунке 1)

7.18.1 Вывод из эксплуатации E/E/PE СБЗС-систем должен осуществляться таким образом, чтобы функциональная безопасность объекта не снижалась из-за обстоятельств, возникающих во время вывода из эксплуатации этих систем, систем управления УО и после их завершения.

7.18.2 Лицами, ответственным за безопасность здания или сооружения в этот период времени, должны быть приняты дополнительные защитные меры, компенсирующие повышение риска, обусловленного выводом из эксплуатации данной E/E/PE СБЗС-системы.

7.18.3 Перед выводом из эксплуатации одной из E/E/PE СБЗС-систем должен быть проведен анализ влияния, который должен включать в себя оценку влияния действий по выводу из эксплуатации этой системы на функциональную безопасность любой другой E/E/PE СБЗС-системы и системы управления УО.

При анализе влияния должны быть также учтены смежные УО и их влияние на E/E/PE СБЗС-системы. Оценка влияния должна включать анализ опасностей и рисков, которые могут возникнуть на последующих стадиях полного жизненного цикла E/E/PE СБЗС-систем или жизненных циклов аппаратных средств либо программного обеспечения.

7.18.4 Утилизация E/E/PE СБЗС-систем и управляемого оборудования должна осуществляться в соответствии с требованиями экологической безопасности.

7.18.5 Результаты действий, указанных в 7.18.1 — 7.18.4, должны быть документированы.

7.18.6 Стадии вывода из эксплуатации или ликвидации E/E/PE СБЗС-систем должны быть инициированы исключительно на основании санкционированного запроса или заявки в соответствии с процедурами по управлению функциональной безопасностью, приведенными в разделе 6.

7.18.7 Разрешение на осуществление требуемого вывода E/E/PE СБЗС-систем из эксплуатации должно выдаваться на основании результатов анализа влияния.

7.18.8 До вывода из эксплуатации должен быть подготовлен план, который должен включать процедуры по отключению и демонтажу E/E/PE СБЗС-систем.

7.18.9 Если какие-либо действия по выводу из эксплуатации оказывают влияние на функциональную безопасность любой другой E/E/PE СБЗС-системы, эти действия должны начинаться с возврата к соответствующей стадии полного жизненного цикла такой системы, жизненного цикла аппаратных средств или программного обеспечения. Затем должны быть осуществлены все последующие стадии в соответствии с процедурами, определенными в настоящем стандарте для заданных уровней полноты безопасности для E/E/PE СБЗС-систем.

7.18.10 Если стадия вывода из эксплуатации E/E/PE СБЗС-системы совпадает со стадией вывода из эксплуатации объекта, то требования к функциональной безопасности этой системы на этой стадии могут отличаться от требований к функциональной безопасности, предусмотренных для стадии эксплуатации.

7.18.11 Должна формироваться и сохраняться в хронологическом порядке документация, содержащая документальные подробности действий по выводу из эксплуатации E/E/PE СБЗС-систем и ссылки на план, используемый для действий по выводу из эксплуатации, а также на анализ влияния.

7.19 Верификация E/E/PE СБЗС-систем

7.19.1 Для каждой стадии жизненного цикла E/E/PE СБЗС-систем должна быть проведена верификация с представлением свидетельств, полученных с помощью проверки, анализа и/или испытаний того, что для каждой стадии полного жизненного цикла E/E/PE СБЗС-систем результаты соответствуют всем целям и требованиям, определенным для этой стадии.

7.19.2 Верификация должна осуществляться в соответствии с планом по верификации.

7.19.3 В плане верификации должны быть документированы критерии, методы, аппаратура и средства, предназначенные для использования в действиях по верификации, или даны ссылки на них.

7.19.4 При выборе технических средств и методов для проведения верификации и степени независимости лиц (отделов, организаций), осуществляющих действия по верификации должны быть учтены:

- степень ответственности, опасности и технической сложности объектов, в которых применены E/E/PE СБЗС-системы;
- состав и число систем в проекте;
- степень сложности E/E/PE СБЗС-систем;
- степень новизны разработки;
- степень новизны технологии.

Примечание — Чем более сложный и объемный проект, чем выше степень новизны разработки и технологии E/E/PE СБЗС-систем, чем выше степень ответственности, опасности и технической сложности зданий и сооружений, тем более жесткими должны быть требования к средствам и методам проведения верификации и степени независимости лиц (отделов, организаций), осуществляющих действия по верификации.

7.19.5 Должна быть собрана и документирована информация о действиях по верификации как доказательство того, что стадия верификации во всех отношениях удовлетворительно завешена.

8 Оценка функциональной безопасности

8.1 Для оценки функциональной безопасности E/E/PE СБЗС-систем должны быть проведены исследования и получены подтверждения того, что всеми установленными в зданиях и сооружениях E/E/PE СБЗС-системами достигнута требуемая функциональная безопасность.

8.2 Для осуществления оценки функциональной безопасности E/E/PE СБЗС-систем с целью получения заключения о достижении всеми E/E/PE СБЗС-системами требуемой функциональной безопасности должны быть назначены одно лицо или большее число лиц.

8.3 Лица, осуществляющие оценку функциональной безопасности, должны иметь доступ ко всем лицам, вовлеченным в любые действия полного жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска и ко всей существенной информации и оборудованию (как аппаратным средствам, так и программному обеспечению), а также к внешним средствам уменьшения риска.

8.4 Оценка функциональной безопасности должна быть применена ко всем стадиям полного жизненного цикла E/E/PE СБЗС-систем зданий и сооружений, жизненных циклов аппаратных средств и программного обеспечения, а также внешних средств уменьшения риска. Лица, проводящие оценку функциональной безопасности, должны рассматривать осуществляемые действия и результаты, полученные в течение каждой стадии жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска исключительно в рамках целей и требований установленных настоящим стандартом.

8.5 Оценка функциональной безопасности должна осуществляться на всех стадиях полного жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска, но может быть осуществлена после ряда стадий жизненного цикла при условии, что оценка функциональной безопасности проводится до появления определенных опасностей.

8.6 Если для разработки или оценки любых действий на стадиях жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска используются инструменты (например, системы компьютерного проектирования CAD/CAM, измерительные приборы и оборудование), они должны стать предметом оценки функциональной безопасности.

При определении степени жесткости предъявляемых к ним требований должно быть оценено их влияние на функциональную безопасность E/E/PE СБЗС-систем.

8.7 В ходе выполнения оценки функциональной безопасности E/E/PE СБЗС-систем должны быть исследованы и оценены:

- работа, проведенная с момента проведения предыдущей оценки функциональной безопасности до текущего момента времени, которая должна охватывать предыдущие стадии жизненного цикла систем, и ее результаты;
- планы или стратегия осуществления дальнейшей оценки функциональной безопасности для жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска;
- рекомендации предыдущей оценки функциональной безопасности и степень выполнения этих рекомендаций.

8.8 Действия по оценке функциональной безопасности для различных стадий жизненного цикла E/E/PE СБЗС-систем, жизненного цикла аппаратных средств и программного обеспечения, внешних средств уменьшения риска должны быть последовательными и запланированными.

8.9 Планом осуществления оценки функциональной безопасности должны быть определены:

- лица, осуществляющие оценку функциональной безопасности;
- результаты каждой оценки функциональной безопасности;
- рамки оценки функциональной безопасности.

8.10 При установлении рамок оценки функциональной безопасности должны быть определены:

- документы, которые используются для каждого действия по оценке, их статус;
- лица, вовлеченные в действия по обеспечению безопасности;
- требуемые ресурсы;
- уровень жесткости требований к независимости лиц, отделов, организаций, осуществляющих оценку функциональной безопасности.

Примечание — Привлечение к оценке функциональной безопасности независимого лица — наименее жесткое требование независимости, привлечение независимой организации — наиболее жесткое требование;

- компетентность лиц, осуществляющих оценку функциональной безопасности.

8.11 До осуществления оценки функциональной безопасности план по оценке функциональной безопасности должен быть согласован с теми лицами, отделами, организациями, которые осуществляют оценку функциональной безопасности и лицами, ответственными за управление функциональной безопасностью на оцениваемых стадиях жизненного цикла E/E/PE СБЗС-систем.

8.12 При завершении оценки функциональной безопасности должны быть выработаны рекомендации по принятию, квалифицированному принятию или отклонению итогов оценки (2/3 принимающих решение).

8.13 Лица, осуществляющие оценку функциональной безопасности, должны быть компетентными для совершаемых действий. Для оценки компетентности должны быть учтены факторы, приведенные в приложении Б.

8.14 Минимальный уровень жесткости требований к независимости лиц, подразделений, организаций, которые осуществляют оценку функциональной безопасности, следует определять в зависимости от возможных последствий реализации опасного события и от целевого уровня полноты безопасности системы с использованием таблиц 3 и 4.

Примечание — Типичными последствиями могут быть: последствие A — незначительный вред (например, временная потеря функции); последствие B — серьезный долговременный вред, причиненный одному или более физическим лицам, смерть одного человека; последствие C — смерть нескольких человек; последствие D — гибель очень большого числа людей (см. ГОСТ Р 53195.1, приложение Б).

Таблица 3 — Уровень жесткости требований к независимости лиц, отделов, организаций, осуществляющих оценку функциональной безопасности (стадии 1 — 10 и 14 — 18 жизненного цикла E/E/PE СБЗС-систем) в зависимости от последствий опасного события

Лицо, отдел, организация	Критерий выбора жесткости требований к независимости лиц, отделов, организаций для последствий			
	A	B	C	D
Независимое лицо	КР	КР[1]	НР	НР
Независимое подразделение	—	КР[2]	КР[1]	НР
Независимая организация	—	—	КР[2]	КР

Таблица 4 — Уровень жесткости требований к независимости лиц, отделов, организаций, осуществляющих оценку функциональной безопасности (стадии 11 жизненного цикла E/E/PE СБЗС-систем) в зависимости от целевого уровня полноты безопасности

Лицо, отдел, организация	Критерий выбора жесткости требований к независимости лиц, отделов, организаций для уровня полноты безопасности			
	SIL 1	SIL 2	SIL 3	SIL 4
Независимое лицо	КР	КР[1]	НР	НР
Независимое подразделение	—	КР[2]	КР[1]	НР
Независимая организация	—	—	КР[2]	КР

Обозначения критериев выбора в таблицах 3 и 4:

КР — уровень независимости крайне рекомендованный, как минимум, для указанного в таблице 3 последствия или указанного в таблице 4 уровня полноты безопасности. Если принимается более низкий уровень независимости, то должно быть приведено детальное логическое обоснование, почему не принят уровень КР;

НР — уровень независимости, недостаточный и положительно не рекомендованный для указанного в таблице 3 последствия или указанного в таблице 4 уровня полноты безопасности. Если принимается этот уровень, то должно быть приведено детальное логическое обоснование, почему он принят;

— — уровень независимости, не имеющий никакой рекомендации, ни за, ни против использования.

8.15 До применения таблицы 3 должны быть определены категории последствий в случае отказа E/E/PE СБЗС-систем, аппаратуры или программного обеспечения, внешних средств уменьшения риска, когда требуется их работа.

8.16 Приведенные в таблицах 3 и 4 уровни независимости КР[1] или КР[2] (но не оба одновременно) должны выбираться с учетом следующих условий.

Если применен уровень независимости КР[1], то уровень КР[2] должен читаться как не требуемый; если применен уровень КР[2], то уровень КР[1] должен читаться как НР (не рекомендованный).

Уровень КР[2] следует выбирать вместо уровня КР[1] в случаях, когда

- на основании предыдущего опыта работы с аналогичным проектом E/E/PE СБЗС-систем обнаружены недостатки;
- здание или сооружение имеет более высокую степень ответственности, опасности или технической сложности;
- разрабатываемый проект E/E/PE СБЗС-систем имеет бóльшую степень сложности;
- имеется бóльшая степень новизны разработки E/E/PE СБЗС-систем;
- имеется бóльшая степень новизны технологии;
- имеются недостатки или пробелы стандартизации по отношению к деталям проекта.

8.17 Минимальный уровень независимости лиц, отделов, организаций, приведенный в таблице 4, должен быть отнесен к функции безопасности, выполняемой E/E/PE СБЗС-системой, имеющей наивысший уровень полноты безопасности SIL 4.

Приложение А
(справочное)

Перечень и идентификация документации

Для идентификации рабочих, прилагаемых и иных документов, а также документов, создаваемых на различных стадиях жизненного цикла СБЗС-систем, следует применять маркировку, приведенную в таблицах А.1 — А.3.

Т а б л и ц а А.1 — Рекомендуемый перечень и маркировка основных комплектов рабочих чертежей для проекта здания и сооружения

Наименование основного комплекта для разделов	Маркировка
Противопожарные автоматизированные системы*	АП
Автоматизированная система управления активной противопожарной защиты*	АПМ
Автоматизированная система противодымной вентиляции*	АПВ
Автоматизированная система спринклерного пожаротушения*	АПС
Автоматизированная система общеобменной вентиляции	АОВ
Автоматизация систем водопровода и канализации	АВК
Автоматизация теплового пункта	АТП
Наружные сети связи	НСС
Наружные сети связи телефонизации	НСС.1
Наружные сети связи радиотрансляции	НСС.2
Наружные сети выделенной связи	НСВ
Наружные сети телевидения	НСТ
Наружные сети объединенной диспетчерской системы	НСД
Наружные сети систем безопасности	НСБ
Объединенные комплексные наружные сети (телевидения, диспетчеризации и др.)	НСО
Информационные наружные сети	НСИ
Системы и комплексы мониторинга*	СМ
Структурированные системы мониторинга и управления инженерными системами зданий и сооружений*	СМ1
Системы мониторинга деформационного состояния конструкций зданий и сооружений*	СМ2
Системы экологического мониторинга*	СМ3
Система контроля соффузионно-карстовых явлений*	СМ4
Комплекс внутренних сетей и систем связи для административных, общественных и высотных многофункциональных зданий и сооружений	СС1
Внутренние сети связи	СС1.1
Учрежденческие телефонные станции	СС1.2
Структурированные кабельные системы и выделенные сети*	СС1.3
Системы оперативной и специальной чрезвычайной связи*	СС1.4
Системы диспетчерской (технологической) телефонной связи	СС1.4.1
Системы оперативной технологической радиосвязи	СС1.4.2
Системы обнаружения людей*	СС1.4.3

Окончание таблицы А.1

Наименование основного комплекта для разделов	Маркировка
Системы оперативной чрезвычайной телефонной связи*	СС1.4.4
Системы громкоговорящей связи	СС1.4.5
Кабельпроводы и закладные устройства для внутренних сетей связи	СС1.5
Узлы связи и коммутации	СС1.7
Комплекс внутренних сетей и систем связи для жилых домов и встроенно-пристроенных помещений	СС2
Телефонные сети (для жилых домов)	СС2.1
Автоматические телефонные станции (для жилых домов)	СС2.2
Выделенные сети (для жилых домов)	СС2.3
Радиотрансляция (для жилых домов)	СС2.4
Кабельпроводы и закладные устройства для внутренних сетей связи	СС2.5
Системы специального назначения	СН
Системы электрочасификации	СН1
Системы управления гостиницей	СН2
Автоматизированные системы управления товарооборотом	СН3
Системы контроля хищений в торговых объектах*	СН4
Информационно-расчетные системы (безналичной оплаты за предоставленные услуги, в т. ч. за питание в школах)	СН5
Автоматизированные системы школ «Карта учащегося»	СН6
Технические средства обучения	СН7
Системы пылеудаления	СН8
Пневмопочта	СН9
Системы и комплексы мониторинга	СМ
Структурированные системы мониторинга и управления инженерными системами зданий и сооружений*	СМ1
Системы мониторинга деформационного состояния конструкций зданий и сооружений*	СМ2
Системы экологического мониторинга*	СМ3
Система контроля соффузионно-карстовых явлений*	СМ4
* E/E/PE СБЗС-система.	

При маркировке комплектов рабочих чертежей других систем рекомендуется использовать буквенные обозначения (не более трех прописных букв). Для обозначения расширения групповых систем следует использовать арабские цифры, отделенные от буквенного обозначения точкой. Для дальнейшего расширения обозначения систем в группе необходимо использовать арабские цифры, отделенные от цифрового обозначения группы точкой.

Таблица А.2 — Рекомендуемые маркировки прилагаемых документов

Наименование прилагаемого документа	Маркировка
Рабочие чертежи индивидуальных изделий	И
Рабочие чертежи узлов, разработанные для данного проекта, и установочные чертежи	У

Окончание таблицы А.2

Наименование основного комплекта для разделов	Маркировка
Конструктивные и установочные чертежи	К
Чертежи общего вида нетиповых конструкций и нестандартного инженерного или технологического оборудования и задания предприятию-изготовителю	Н
Спецификация оборудования	СО
Ведомость потребности в материалах	ВМ
Ведомость объемов строительных и монтажных работ	ВР

Таблица А.3 — Рекомендуемые маркировки других документов

Наименование документа	Маркировка
Сборник спецификации оборудования	ССО
Сводная потребность в материалах	СВМ
Сборник ведомостей объемов строительных и монтажных работ	СВР
Пояснительная записка	ПЗ
Технические условия	ТУ
Специальные технические условия	СТУ
Технические требования	ТТ
Расчеты	РР
Чертеж формы (опалубочный чертеж)	ФЧ
Ведомость расхода стали	РС
Номенклатура изделий	НИ
Справочный материал	СМ
Патентный формуляр	ПФ
Карта технического уровня и качества продукции	КУ
Техническое описание	ТО

Таблица А.4 — Рекомендуемые виды документов, создаваемых на разных стадиях жизненного цикла объекта или СБЗС-систем

Тип документа	Содержание документа (действие или объект)	Пример наименования документа
Перечень	Функций, характеристик, действий	Перечень требований к полноте безопасности
Описание	Функции, проекта, характеристики	Описание функции безопасности
Инструкция	Когда и как выполнять работы	Инструкция оператора
План	Когда, как и кем должны быть выполнены работы	План технического обслуживания
Список	Содержание списка	Список кодов
Журнал	Событий в хронологической регистрационной форме	Журнал отказов, журнал проведения инструктажа
Отчет	Результаты действий	Отчет об испытаниях
Запрос	Описание запрашиваемых действий	Запрос на видоизменение системы управления доступом

Приложение Б
(справочное)

Пример структуры документации

Б.1 Структура документа

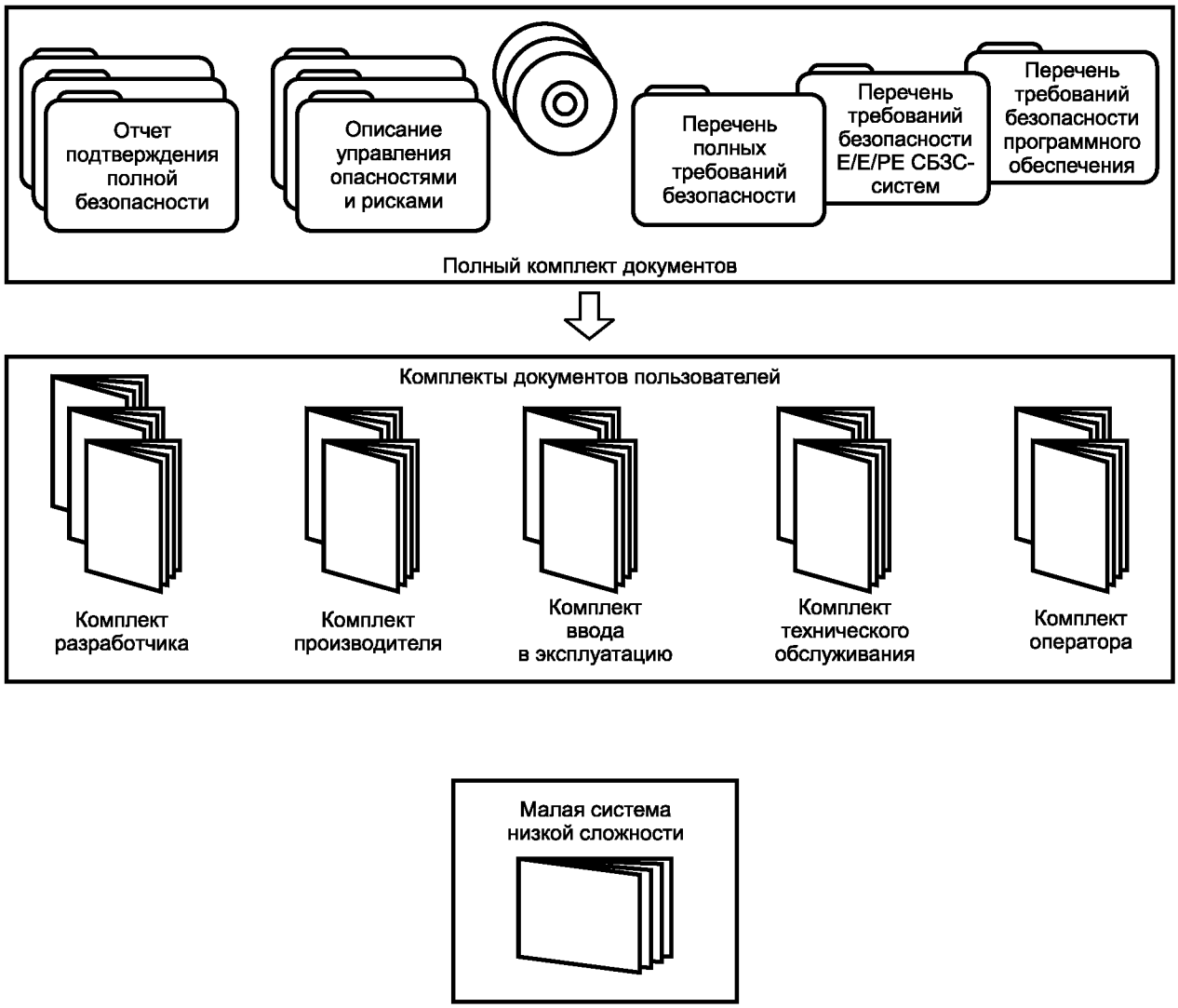


Рисунок Б.1 — Пример структурирования информации в комплекты документов для групп пользователей

Б.2 Регистрация документа

Регистрационный признак документа должен включать в себя следующую информацию:
- номер чертежа или документа;
- индекс пересмотра;
- код обозначения документа;
- наименование документа;
- дату пересмотра;
- обозначение носителя информации.

Приложение В
(справочное)

Компетентность лиц

Все лица, вовлеченные в любые действия, связанные с обеспечением жизненного цикла СБЗС-систем, аппаратных средств, программного обеспечения, внешних средств уменьшения риска, включая действия по управлению, должны иметь технические знания, опыт и квалификацию, соответствующие служебным обязанностям, которые они должны выполнять.

Для каждого конкретного применения должны быть оценены практическая подготовка, опыт и квалификация всех лиц, вовлеченных в деятельность по обеспечению безопасности зданий и сооружений и связанных с их безопасностью систем в течение полного жизненного цикла объекта и систем, включая деятельность по управлению функциональной безопасностью.

При оценке компетентности лиц должны быть учтены следующие факторы:

а) инженерные и технические знания в соответствующей области применения;

б) инженерные и технические знания, соответствующие технологии (например, электрическая, электронная, электронная программируемая, программирование);

в) инженерные знания в области технических систем и средств обеспечения безопасности, соответствующих технологий;

г) инженерные знания в области комплексных систем безопасности зданий и сооружений;

д) знание систем правового и технического регулирования в области безопасности зданий и сооружений;

е) последствия в случае отказов E/E/PE СБЗС-систем и внешних средств уменьшения риска зданий и сооружений; чем большая тяжесть последствий, тем более строгими должны быть перечень требований и оценка компетентности;

ж) уровень полноты безопасности E/E/PE СБЗС-систем и внешних средств уменьшения риска; чем больший уровень полноты безопасности, тем более строгими должны быть перечень требований и оценка компетентности;

и) новизна разработки, процедур разработки или применения; чем более новые и непроверенные разработки, процедуры разработки или применения, тем более строгими должны быть перечень требований и оценка компетентности;

к) предыдущий опыт и существенность его применения для выполнения определенных служебных обязанностей; чем выше требуемые уровни компетентности, тем меньшим должно быть различие между компетентностью, полученной от предыдущего опыта, и компетентностью, требуемой для выполнения определенных обязанностей;

л) достаточность квалификации для выполнения конкретных обязанностей.

Сведения об обучении, тренинге, опыте и квалификации всех лиц, вовлеченных в любую деятельность по обеспечению полного жизненного цикла безопасности, жизненных циклов E/E/PE СБЗС-систем, СБЗС и внешних средств уменьшения риска должны быть документированы в хронологическом порядке.

УДК 621.5:814.8:006.364	ОКС 13.100; 13.110; 13.200; 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, общие требования

Редактор *Н. О. Грач*
Технический редактор *В. Н. Прусакова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 10.03.2009. Подписано в печать 06.05.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. 4,18. Уч.-изд. л. 3,90. Тираж 253 экз. Зак. 439.

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

gost.e-ecolog.ru