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

МЕЖГОСУДАРСТВЕННЫЙ
СТАНДАРТ

**ГОСТ
34332.2—
2017**

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 2

Общие требования

**(IEC 61508-1:2010, NEQ)
(ISO/IEC Guide 51:2014, NEQ)**

Издание официальное

**Москва
Стандартинформ
2018**

Предисловие

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

Сведения о стандарте

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

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

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

За принятие проголосовали:

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

4 Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 830-ст межгосударственный стандарт ГОСТ 34332.2—2017 введен в действие в качестве национального стандарта Российской Федерации с 1 марта 2019 г.

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

IEC 61508-1:2010 «Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 1. Общие требования» («Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements», NEQ);

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

6 ВВЕДЕН ВПЕРВЫЕ

7 Настоящий стандарт подготовлен на основе применения ГОСТ Р 53195.2—2008*

* Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 830-ст ГОСТ Р 53195.2—2008 отменен с 1 марта 2019 г.

Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст этих изменений — в ежемесячном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 3
5 Требования 3
6 Управление функциональной безопасностью 5
7 Полный жизненный цикл 7
8 Оценка функциональной безопасности 24
Приложение А (справочное) Пример структуры документации 28
Библиография 33

Введение

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

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

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

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

В настоящем стандарте установлены общие требования, относящиеся к функциональной безопасности электрических, электронных, программируемых электронных систем, связанных с безопасностью зданий и сооружений (Э/Э/ПЭ СБЗС систем), и процедурам, которые должны быть выполнены на стадиях жизненного цикла этих систем для достижения и поддержания их функциональной безопасности. Стандарт ориентирован на обеспечение соблюдения требований безопасности зданий и сооружений, в том числе объектов транспортных инфраструктур, установленных техническими регламентами Таможенного союза [1]—[3], а также Техническим регламентом Евразийского экономического союза [4] (после его вступления в силу) и в развитие базовых требований этих технических регламентов.

Настоящий стандарт распространяется на Э/Э/ПЭ СБЗС системы и составляющие этих систем, включая сенсоры, исполнительные устройства и интерфейс «человек — машина». Он рассчитан на любой диапазон сложности Э/Э/ПЭ СБЗС систем и ориентирован на комплексное обеспечение безопасности зданий и сооружений.

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

Часть 1. Основные положения;

Часть 3. Требования к системам;

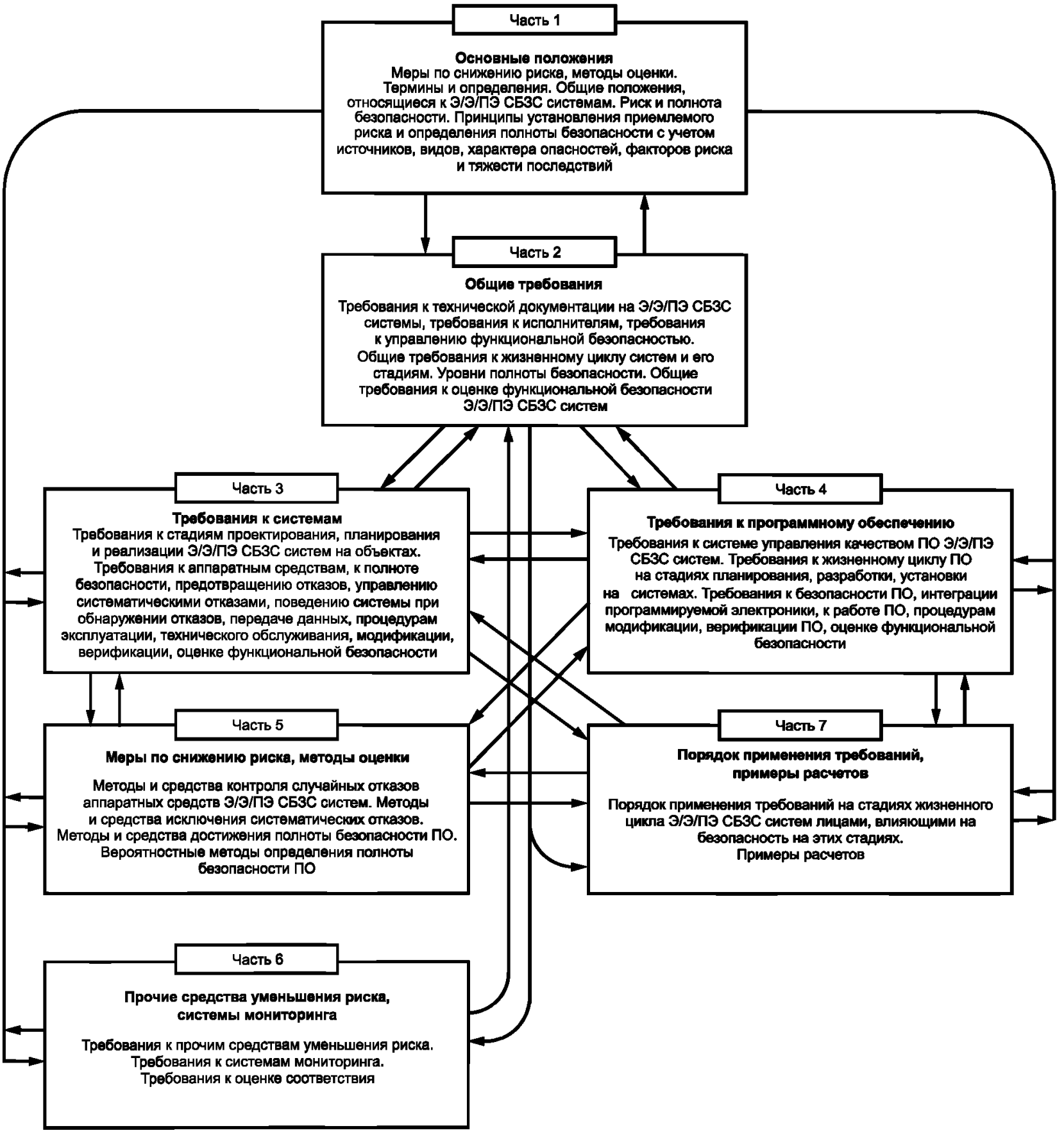
Часть 4. Требования к программному обеспечению;

Часть 5. Меры по снижению риска, методы оценки;

Часть 6. Прочие средства уменьшения риска, системы мониторинга;

Часть 7. Порядок применения требований, примеры расчетов.

Структура комплекса стандартов приведена ниже.


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

ПОПРАВКИ, ВНЕСЕННЫЕ В МЕЖГОСУДАРСТВЕННЫЕ СТАНДАРТЫ

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

МКС 13.100
13.110
13.200
13.220
13.310
13.320
91.120.99

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

В каком месте	Напечатано	Должно быть
Предисловие. Пункт 7	ГОСТ Р 53195.2—2008*	ГОСТ Р 53195.2—2008
Сноска — *	———— * Приказом Федерального агентства по техническому регулированию и метрологии от 23 октября 2018 г. № 830-ст ГОСТ Р 53195.2—2008 отменен с 1 марта 2019 г.	—

(ИУС № 5 2020 г.)

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

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ ЗДАНИЙ И СООРУЖЕНИЙ

Часть 2

Общие требования

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

Дата введения — 2019—03—01

1 Область применения

1.1 Настоящий стандарт:

- устанавливает общие требования к документации, к функциональной безопасности электрических, электронных, программируемых электронных (далее — Э/Э/ПЭ) систем, связанных с безопасностью зданий и сооружений (далее — СБЗС систем);
- устанавливает общие требования к полному жизненному циклу (далее — ЖЦ) Э/Э/ПЭ СБЗС систем, отдельным его стадиям и этапам, а также процедурам, применяемым на этих стадиях и этапах;
- определяет основные целевые уровни полноты безопасности (далее — УПБ) функций безопасности, которые должны быть реализованы Э/Э/ПЭ СБЗС системами.

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

1.3 Настоящий стандарт не распространяется на Э/Э/ПЭ СБЗС систему, которая является единственной одиночной системой, способной осуществить необходимое снижение риска на объекте, и требуемая полнота безопасности этой системы ниже, чем определено УПБ 1 — самым низким уровнем, приведенным в таблицах 1 и 2.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.051—2013 Единая система конструкторской документации. Электронные документы. Общие положения

ГОСТ 21.110—2013 Система проектной документации для строительства. Спецификация оборудования, изделий и материалов

ГОСТ ISO 9001—2011 Системы менеджмента качества. Требования

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

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 ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежегодного информационного указателя «Национальные стандарты» за текущий год. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 34332.1, а также следующие термины с соответствующими определениями:

3.1 **независимая организация** (independent organization): Отдельная организация, выполняющая оценку или аудит функциональной безопасности, не имеющая общего управления и ресурсов с организациями, несущими ответственность за процессы, осуществляемые в течение конкретной стадии ЖЦ системы, связанной с безопасностью здания или сооружения, или ее составляющей.

3.2 **независимое лицо** (independent person): Лицо, проводящее оценку или аудит функциональной безопасности, не зависимое и не связанное с действиями, происходящими во время конкретной стадии ЖЦ системы, связанной с безопасностью здания или сооружения, 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, независимое и не связанное с подразделениями, отвечающими за действия, осуществляемые в течение конкретной стадии ЖЦ, связанной с безопасностью здания и сооружения, или ее составляющей.

3.4 **полная функция безопасности** (overall safety function): Функция безопасности программируемой электронной системы, связанной с безопасностью, обеспеченная одновременным действием АС и ПО этой системы.

3.5 **прослеживание** (tracing): Процесс сбора, обработки и сохранения в хронологическом порядке сведений о продукции и ее составляющих.

Примечание — В перечень сведений входят сведения о происхождении продукции, ее составляющих, из которых она была создана, процессов обработки, условиях ее транспортирования и хранения, которым она подвергалась к моменту ее приобретения потребителем.

3.6 **режим работы связанной с безопасностью системы**; режим работы СБ системы (operate mode of safety-related system): Режим работы СБ системы по отношению к частоте запросов к ней, который может быть либо режимом с низкой частотой запросов, когда частота запросов на выполнение 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 на выполнение операции связанной с безопасностью системой превышает один раз в год или превышает более чем в два раза частоту, зарегистрированную во время контрольных испытаний.

3.7 **связанное с безопасностью зданий и сооружений программное обеспечение**; СБЗС ПО: ПО Э/Э/ПЭ СБЗС систем, которое используется для реализации функции или функций безопасности систем, связанных с безопасностью зданий и (или) сооружений.

3.8 **управление конфигурацией** (configuration management): Процесс идентификации составляющих (компонентов) рассматриваемых систем для управления изменением этих составляющих, связей между ними, поддержания преемственности и прослеживания на протяжении всего их ЖЦ.

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

Примечание — УПБ 4 характеризует наибольшую полноту безопасности ПО, УПБ 1 соответствует наименьшей полноте безопасности ПО.

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

Примечание — Целевая мера 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 непрерывным запросом.

3.11

электронный носитель: Материальный носитель, используемый для записи хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники.

[ГОСТ 2.051—2013, пункт 3.1.9]

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и обозначения:

АС — аппаратное(ые) средство(а);

ЕАЭС — Евразийский экономический союз;

ЖЦ — жизненный цикл;

КСБ — комплексная система безопасности;

ПО — программное обеспечение;

СБ система — связанная с безопасностью система;

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

УО — управляемое оборудование;

УПБ — уровень полноты безопасности;

УПБ ПО — уровень полноты безопасности программного обеспечения;

Э/Э/ПЭ — электрическая(ое), электронная(ое), программируемая электронная(ое) (по отношению к системе, оборудованию или компоненту);

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

BIM — информационное моделирование в строительстве (от английского «Building Information Modeling»).

5 Требования

5.1 Соответствие требованиям настоящего стандарта

5.1.1 Требования настоящего стандарта считают выполненными, если представлены доказательства удовлетворения требований и достижения всех целей, определенных в каждом разделе и подразделе стандарта. При этом должны быть учтены следующие факторы: природа и характер опасностей, снижение риска и тяжести последствий опасных событий, УПБ, типы использованных технологий, размеры системы, число используемых команд, физическая среда применения, новизна разработки.

5.1.2 В качестве доказательственных материалов используют выходные данные, подлежащие документированию, предусмотренные разделом 7, верифицированные в соответствии с 7.19 и содержащие результаты оценки функциональной безопасности, проведенной в соответствии с разделом 8.

5.1.3 На стадиях проектирования, реализации (установки и монтажа на объекте), ввода в действие, эксплуатации и видоизменения (модификации) Э/Э/ПЭ СБЗС систем лицам, несущим ответственность за безопасность на соответствующей стадии или стадиях ЖЦ, по их запросу предоставляют информацию, предусмотренную в 7.7, 7.15—7.17 и 7.19.

5.1.4 В рамках настоящего стандарта учитывают положения Руководства ИСО/МЭК 51 [1] по аспектам безопасности и требования ГОСТ ISO 9001.

5.2 Требования к документации

5.2.1 Документированию подлежит информация, необходимая для эффективного представления всех стадий полного ЖЦ Э/Э/ПЭ СБЗС систем, АС и ПО этих систем, а также информация, необходимая для эффективного осуществления: управления функциональной безопасностью в соответствии с разделом 6, верификации в соответствии с 7.18, действий по обеспечению функциональной безопасности и ее оценке в соответствии с разделом 8.

5.2.2 Документацию допускается представлять на любом носителе (например, на электронном носителе, на бумаге, пленке или другом носителе информации).

Документация может быть также представлена в форме файлов, действующих под управлением программы информационной поддержки ЖЦ продукции.

Примечание — На стадиях и этапах от разработки концепции до завершения проектирования Э/Э/ПЭ СБЗС систем в качестве программ информационной поддержки ЖЦ продукции часто используют программы информационного моделирования в строительстве (*BIM*).

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

5.2.4 В проектной документации на здание или сооружение должны быть отражены мероприятия по комплексному обеспечению безопасности объектов с применением Э/Э/ПЭ СБЗС систем, а в проектной документации на особо опасные, технически сложные, уникальные объекты и объекты повышенного уровня ответственности — мероприятия по комплексному обеспечению безопасности и антитеррористической защищенности объектов с применением этих систем. Для обеспечения действий по реализации ЖЦ этих систем и удобства управления их функциональной безопасностью на стадиях ЖЦ эти мероприятия следует оформлять в проектной документации в виде отдельного раздела, подраздела или подподраздела.

5.2.5 Состав и число Э/Э/ПЭ СБЗС систем или подсистем для комплексного обеспечения безопасности для конкретного здания или сооружения определяются проектировщиком на стадии проектирования.

5.2.6 Документация, относящаяся к Э/Э/ПЭ СБЗС системам, со всеми утвержденными изменениями должна быть сохранена на протяжении всего ЖЦ систем и объекта. Ее создают, обрабатывают, представляют и сохраняют таким образом, чтобы выполнялись требования, установленные в 5.7—5.10.

5.2.7 В документацию включают текстовую и/или графическую информацию для каждой стадии полного ЖЦ Э/Э/ПЭ СБЗС систем и их составляющих (ЖЦ их АС и ПО), достаточную для реализации составляющих стадий ЖЦ и действий по верификации в соответствии с 7.19, управлению функциональной безопасностью в соответствии с разделом 6, оценки 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), обеспечивающие доступ к информации, предусмотренный настоящим стандартом, индекс пересмотра или номер версии для обеспечения возможности идентификации различных версий документа.

5.2.9 Документацию структурируют таким образом, чтобы обеспечить возможность лицам, осуществляющим действия по обеспечению безопасности на стадиях ЖЦ Э/Э/ПЭ СБЗС систем, поиска существенной информации. Документацию компонуют в комплекты, удобные для пользования этими лицами.

Примечания

1 Примеры перечней и идентификация проектной и рабочей документации и документации, выпускаемой на других стадиях ЖЦ Э/Э/ПЭ СБЗС систем, приведены в приложении А.

2 Структура документации может быть изменена в зависимости от состава, числа Э/Э/ПЭ СБЗС систем, их сложности и организационных требований.

5.2.10 Проверка, внесение изменений, пересмотр, утверждение документации должны быть обеспечены соответствующей системой управления документацией, принятой в организации, не противоречащей ГОСТ ISO 9001 (подраздел 4.2).

6 Управление функциональной безопасностью

6.1 Цели

Цели настоящего раздела состоят:

- в определении организаций, подразделений и лиц, которые несут ответственность за управление функциональной безопасностью, отвечают за Э/Э/ПЭ СБЗС системы, их АС или ПО на одной или нескольких стадиях ЖЦ;
- в определении мероприятий, которые должны быть проведены ими, и обязанностями по управлению функциональной безопасностью.

6.2 Требования к организациям, лицам и процедурам

6.2.1 Организация, ответственная за Э/Э/ПЭ СБЗС систему или за одну или несколько стадий ЖЦ всей системы, ее АС или ПО, должна выделить одно лицо или большее число лиц, несущих полную ответственность:

- за систему и стадии ее ЖЦ;
- за координацию действий, влияющих на безопасность, выполняемых на этих стадиях;
- за взаимодействие между этими стадиями и другими стадиями, выполняемыми другими организациями;
- за выполнение требований 6.2.2—6.2.11 и 6.2.13;
- за координацию оценки функциональной безопасности (см. раздел 8), особенно на тех стадиях, на которых выполнение оценки функциональной безопасности различается, включая взаимодействие, планирование, а также обобщение документации, обоснований и рекомендаций;
- за удостоверение того, что функциональная безопасность достигнута и продемонстрировано соответствие целям и требованиям настоящего стандарта.

Примечание — Ответственность за действия, связанные с безопасностью, за одну или несколько стадий ЖЦ Э/Э/ПЭ СБЗС систем могут быть делегированы другим лицам, в частности, осуществляющим экспертизу. При этом за разные действия могут быть ответственными разные лица. Однако ответственность за координацию и функциональную безопасность всей системы должна принадлежать одному лицу или небольшой группе лиц с достаточным уровнем административного ресурса.

6.2.2 Должны быть определены политика и стратегия достижения функциональной безопасности, а также средства для оценки ее достижения и средства взаимодействия внутри организации в соответствии с руководством по качеству, принятом в организации, не противоречащим требованиям ГОСТ ISO 9001.

6.2.3 Должны быть определены все лица, подразделения и организации, ответственные за выполнение действий на соответствующих стадиях ЖЦ всей системы безопасности, Э/Э/ПЭ СБЗС системы, АС или ПО (включая отдельных лиц, ответственных за верификацию и оценку функциональной безопасности, и, где это необходимо, органы лицензирования и органы регулирования в области безопасности), и их ответственность должна быть полностью и ясно доведена до сведения этих лиц.

6.2.4 Должны быть разработаны процедуры для определения, какая информация будет передаваться между соответствующими сторонами и как эта передача будет осуществляться.

Примечание — Требования к документации см. в разделе 5.

6.2.5 Должны быть разработаны процедуры, предназначенные для обеспечения быстрого исполнения решений и учета рекомендаций, относящихся к Э/Э/ПЭ СБЗС системам, сформированные по результатам:

- анализа опасностей и рисков в соответствии с 7.4;
- оценки функциональной безопасности в соответствии с разделом 8;
- действий по верификации в соответствии с 7.18;
- действий по подтверждению соответствия в соответствии с 7.8 и 7.14;
- управления конфигурацией;
- отчетов и анализа возможных несоответствий по 6.2.6.

6.2.6 Должны быть разработаны процедуры, которые гарантируют, что все обнаруженные опасные события будут проанализированы и что будут выработаны рекомендации по минимизации возможности их повторения.

6.2.7 Должны быть определены требования к периодическому аудиту функциональной безопасности Э/Э/ПЭ СБЗС систем, включая:

- частоту проведения аудита функциональной безопасности;
- уровень независимости стороны, отвечающей за аудит;
- требуемую документацию и программу выполнения аудита.

6.2.8 Должны быть разработаны процедуры для:

- инициирования модификации (видоизменения) Э/Э/ПЭ СБЗС систем в соответствии с 7.17;
- получения разрешения и полномочий на осуществление модификации (видоизменения).

6.2.9 Должны быть:

- разработаны процедуры для поддержания точной информации об опасностях и опасных событиях, функциях безопасности Э/Э/ПЭ СБЗС систем;
- разработаны процедуры для управления конфигурацией Э/Э/ПЭ СБЗС систем на всех стадиях ЖЦ Э/Э/ПЭ СБЗС систем, их АС и ПО, в том числе должны быть:
- установлены этапы на определенных стадиях, на которых должен быть осуществлен формальный контроль конфигурации;
- разработаны процедуры, которые должны быть применены для уникальной идентификации всех составляющих систем (АС и ПО);
- разработаны процедуры для предотвращения использования контрафактных составляющих (комплектующих).

6.2.10 Для службы безопасности объекта, по возможности, должно быть обеспечено соответствующее обучение персонала, и должна быть соответствующая информация для этих целей.

6.2.11 Лица, несущие ответственность за одну или более стадий ЖЦ Э/Э/ПЭ СБЗС системы, АС или ПО должны для тех стадий, за которые они несут ответственность, и в соответствии с процедурами, определенными в 6.2.1—6.2.10, определить все управленческие и технические действия, необходимые для обеспечения достижения, демонстрации и поддержания функциональной безопасности Э/Э/ПЭ СБЗС систем, включая:

- определение мер (методов и средств), которые для этого могут быть использованы.

Примечание — Такие меры представлены в отдельных стандартах;

- действия по оценке функциональной безопасности, а также способ, с помощью которого будет продемонстрировано достижение функциональной безопасности для тех, кто осуществляет ее оценку (см. раздел 8);
- процедуры для анализа эксплуатации и технического обслуживания, в частности:

а) для распознавания систематических отказов, которые могут поставить под угрозу функциональную безопасность, включая процедуры, используемые во время регламентных работ по обнаружению повторяющихся отказов;

б) для сравнения оцениваемой частоты (интенсивности) запросов и частоты (интенсивности) отказов во время эксплуатации и технического обслуживания с соответствующими предположениями, сделанными в ходе разработки системы.

6.2.12 Должны быть разработаны процедуры, гарантирующие, что все лица, ответственность которых определена в 6.2.1 и 6.2.3, имеют соответствующую необходимую компетентность (т. е. обучены, обладают техническими знаниями, опытом и квалификацией), относящуюся к конкретным обязанностям, которые они должны выполнять. В такие процедуры включают требования к актуализации, обновлению и повышению уровня компетентности.

6.2.13 Соответствие компетентности должно быть рассмотрено для конкретной области применения с учетом всех факторов, включая:

- ответственность конкретного лица;
- уровень необходимого надзора;
- возможные последствия в случае отказа Э/Э/ПЭ СБЗС систем;
- уровни полноты безопасности Э/Э/ПЭ СБЗС систем;
- новизна проекта, проектных процедур или области применения;
- предыдущий опыт и его актуальность для конкретных выполняемых обязанностей и используемых технологий;
- тип компетентности, соответствующей обстоятельствам (например, квалификация, опыт, соответствующая подготовка и последующая практика, способность к лидерству и принятию решений);

- инженерные знания, соответствующие области применения и технологии;
- инженерные знания в области безопасности, соответствующие применяемой технологии;
- знание законодательной базы и нормативно-технической базы в области безопасности;
- соответствие квалификации конкретным выполняемым действиям.

6.2.14 Ответственность всех лиц, определенных в 6.2.1, и их компетентность, установленная в 6.2.13, должны быть документально оформлены.

6.2.15 Действия, приведенные в 6.2.1, 6.2.3, 6.2.13, должны быть реализованы, и их выполнение должно быть проконтролировано.

6.2.16 Поставщики, предоставляющие продукцию или услуги организациям, несущим полную ответственность за одну или несколько стадий ЖЦ Э/Э/ПЭ СБЗС системы, АС или ПО (см. 6.2.1), должны поставлять свою продукцию и услуги в соответствии с требованиями этих организаций и должны иметь соответствующую систему управления качеством, не противоречащую требованиям ГОСТ ISO 9001.

6.2.17 Действия, относящиеся к управлению функциональной безопасности, должны быть применены на соответствующих стадиях ЖЦ Э/Э/ПЭ СБЗС системы, ее АС и ПО.

7 Полный жизненный цикл

7.1 Цели и требования

7.1.1 Цели настоящего раздела состоят в структурировании стадий и этапов полного ЖЦ Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска, подлежащих рассмотрению для обеспечения необходимой функциональной безопасности, и в документальном оформлении ключевой информации по безопасности, относящейся к указанным системам и средствам на этих стадиях и этапах ЖЦ.

Базовая структура полного ЖЦ СБЗС систем совместно со стадиями ЖЦ объекта (здания или сооружения), охватывающая основные действия, необходимые для достижения и поддержания требуемой полноты функциональной безопасности Э/Э/ПЭ СБЗС систем, представлена на рисунке 1.

Структура полного ЖЦ Э/Э/ПЭ СБЗС систем конкретного объекта может быть дополнена, сокращена или изменена по отношению к базовой структуре при условии обоснования новой структуры и обеспечения выполнения целей и требований настоящего стандарта.

Примечание — В течение одного ЖЦ объекта может пройти несколько ЖЦ Э/Э/ПЭ СБЗС систем.

7.1.2 Действия, относящиеся к верификации, управлению функциональной безопасностью и ее оценке, не отображенные на рисунке 1, относятся ко всем стадиям ЖЦ Э/Э/ПЭ СБЗС систем, ЖЦ АС и ПО. Они должны быть выполнены, и результаты действий — документированы.

7.1.3 Для каждой конкретной Э/Э/ПЭ СБЗС системы должны быть установлены в документации, создаваемой на разных стадиях ЖЦ, и выполнены все необходимые итерационные действия, относящиеся к определенным стадиям или этапам между стадиями, не отображенным на рисунке 1, в том числе действия, относящиеся:

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

Примечание — Итерационные действия по оценке риска и снижению риска, применяемые на стадиях ЖЦ Э/Э/ПЭ СБЗС систем, приведены в ГОСТ 34332.1 (пункт 7.2.1 и рисунок 4). Они соответствуют действиям, установленным в международном руководстве [5].

7.1.4 При проектировании должно быть проведено структурирование стадий в полном ЖЦ Э/Э/ПЭ СБЗС систем, в которых должны быть установлены соответствующие действия для достижения требуемой функциональной безопасности.

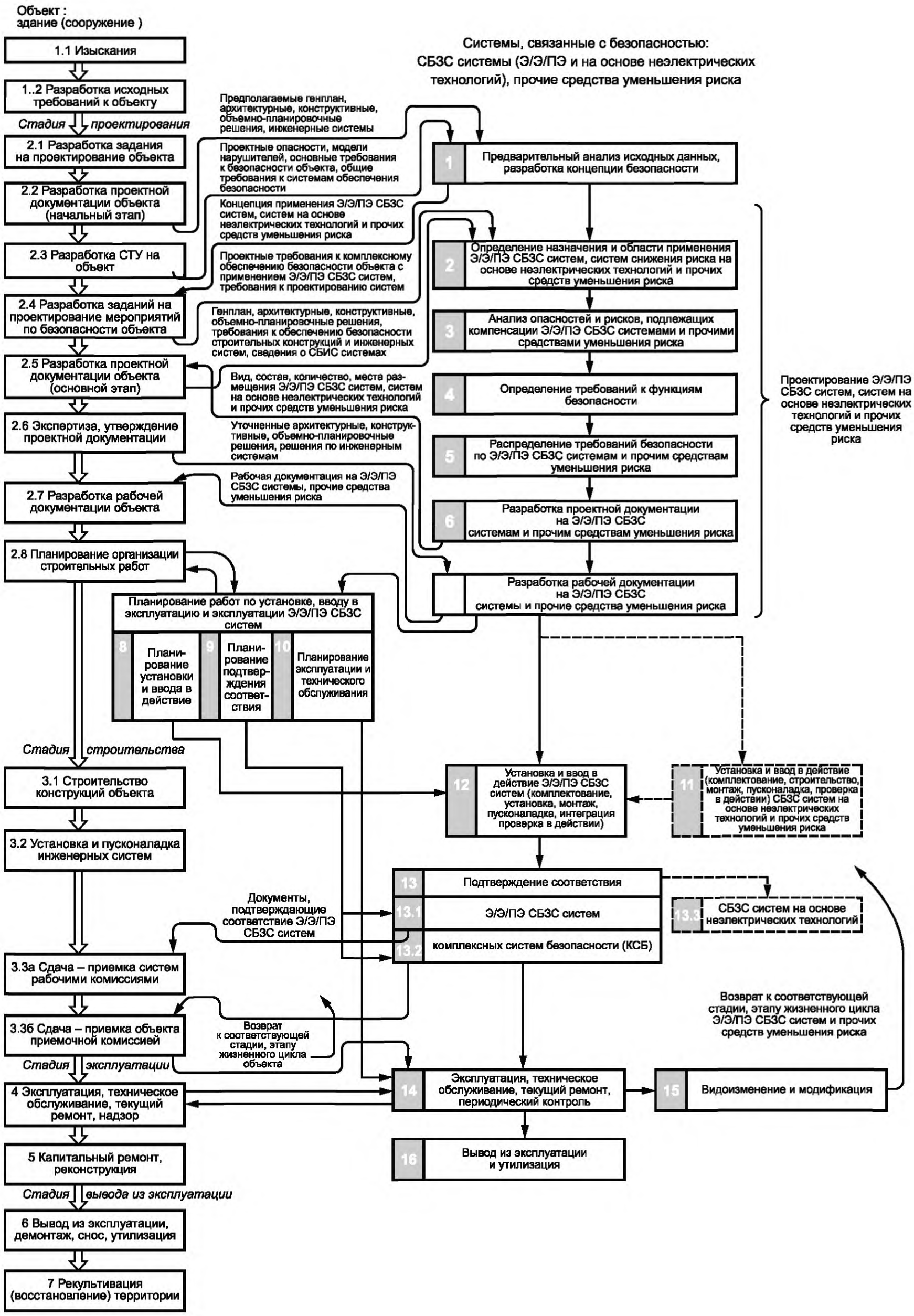


Рисунок 1 — Базовая структура ЖЦ СБЗС систем совместно с ЖЦ объекта

7.1.5 Детальное структурирование стадий и этапов ЖЦ АС и ПО Э/Э/ПЭ СБЗС систем с требованиями к ним может быть установлено в отдельных стандартах на Э/Э/ПЭ СБЗС системы и их ПО.

7.1.6 Информацию, относящуюся к функциональной безопасности Э/Э/ПЭ СБЗС систем, следует документировать в хронологическом порядке на протяжении всего ЖЦ систем.

7.1.7 Требования к управлению функциональной безопасностью (см. раздел 6) следует выполнять параллельно со стадиями полного ЖЦ Э/Э/ПЭ СБЗС систем. Должна быть рассмотрена каждая стадия полного ЖЦ этих систем и должны быть выполнены все соответствующие требования.

7.1.8 Каждая стадия полного ЖЦ Э/Э/ПЭ СБЗС системы должна быть разделена на элементарные действия с указанием для каждой стадии области определения, ее входных данных — входов и результатов — выходов.

7.1.9 Результаты (выходы) каждой стадии полного ЖЦ Э/Э/ПЭ СБЗС систем должны быть проверены (верифицированы) на достижение целей и требований, установленных для каждой стадии в 7.2—7.18.

7.1.10 Для каждой стадии ЖЦ Э/Э/ПЭ СБЗС систем должны быть выполнены требования к верификации, установленные в 7.19.

7.2 Разработка концепции

7.2.1 На этапе разработки концепции СБЗС систем (см. блок 1 на рисунке 1) должны быть рассмотрены и учтены:

- предпроектные предложения по проектированию, реконструкции или капитальному ремонту здания (сооружения) (при их наличии), характеристики объекта, уровень ответственности, предварительные генеральный план, архитектурные, функционально-технологические, объемно-планировочные и конструктивные решения, инженерные системы и УО, предполагаемые для применения в конкретном здании (сооружении), их функции управления и физическое окружение;
- информация о вероятных источниках опасности природного, техногенного и антропогенного характера, проектных опасных воздействиях, моделях нарушителей, моделях угроз с учетом местных условий;
- требования действующих технических регламентов.

Примечания

1 К межгосударственным техническим регламентам по безопасности объектов инфраструктур наземного транспорта относятся технические регламенты Таможенного союза [2]—[4].

2 После вступления в силу к ним будет относиться Технический регламент Евразийского экономического союза [5];

- требования стандартов и сводов правил по безопасности зданий и сооружений, их инженерных систем, общие требования к объемно-планировочным решениям, системам и средствам связи;
- опасности, вызванные взаимодействием каждого 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 заданий на проектирование разделов (подразделов, пунктов) проектной документации.

7.3 Определение области применения

7.3.1 На этапе определения области применения Э/Э/ПЭ СБЗС систем (см. блок 2 на рисунке 1) в целях задания диапазона проектных техногенных, природных, антропогенных опасностей, установленных условиями договора, заданием на проектирование, техническими условиями или специальными техническими условиями (при их наличии), подлежащих компенсации этими 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:

- 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 рисков;
- конкретное оборудование, предполагаемое к установке на объекте, включая УО и системы управления УО;
- системы и подсистемы, связанные с опасностями и риском;

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

- виды опасностей и факторы риска, а также возможная тяжесть последствий опасных событий, приведенные в ГОСТ 34332.1 (раздел 6 и приложения Б, В и Г).

7.3.2 Результаты, полученные в 7.3.1, должны быть документированы.

7.4 Анализ опасностей и рисков

7.4.1 При анализе опасностей и рисков (см. блок 3 на рисунке 1) должны быть учтены требования, установленные условиями договора, заданием на проектирование, техническими условиями или специальными техническими условиями (при их наличии), а также представленные разработчиком(ами) соответствующие разделы проекта объекта с архитектурными, конструктивными, инженерными решениями и уровень остаточного риска, обусловленного этими решениями, с учетом рисков, связанных с системой строительных конструкций и оборудованием 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 АС и ПО Э/Э/ПЭ СБЗС систем;

- риски УО, связанные с опасными событиями.

7.4.3 Должен быть проведен анализ опасностей и рисков, в котором учитывают результаты, полученные в 7.3.1, 7.4.1, 7.4.2. При этом может потребоваться проведение нескольких вариаций анализа опасностей и рисков с различными возможными последовательностями развития опасных событий. Число вариаций анализа определяется проектировщиком Э/Э/ПЭ СБЗС систем.

7.4.4 Должен быть проведен анализ возможности предотвращения опасного события или последовательности опасных событий путем изменения архитектурных, объемно-планировочных, конструктивных и инженерных решений, изменения процесса разработки Э/Э/ПЭ СБЗС систем, видоизменения АС и ПО.

7.4.5 Должны быть определены возможные последствия опасных событий и оценена вероятность их возникновения, в том числе для условий, определенных в 7.4.3.

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

7.4.7 Для выполнения требований 7.4.1—7.4.6 могут быть применены методы количественного или качественного анализа опасностей и риска, приведенные в ГОСТ 34332.1 (приложения Е—Н).

7.4.8 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;

- риск УО;

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

7.4.9 При анализе опасностей и рисков должны быть учтены:

- каждое установленное опасное событие и составляющие (компоненты) Э/Э/ПЭ 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 (интенсивности) запросов и частоты (интенсивности) 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 Э/Э/ПЭ СБЗС системам на предыдущих стадиях их ЖЦ, включая действия по верификации и подтверждению соответствия.

7.4.10 Информация и результаты анализа опасностей и рисков должны быть документированы и сохранены вплоть до вывода Э/Э/ПЭ СБЗС систем из эксплуатации и утилизации.

7.5 Определение требований к функциям безопасности

7.5.1 На этапе определения требований к функциям безопасности (см. блок 4 на рисунке 1) на основе рассмотрения опасных событий, полученных в результате анализа опасностей и рисков, должен быть разработан набор всех необходимых функций безопасности, который представляет собой спецификацию полных требований к полным функциям безопасности.

7.5.2 Если были выявлены угрозы безопасности, то с целью уточнения требований безопасности следует проводить анализ уязвимости.

7.5.3 При использовании СБЗС систем, основанных на неэлектрических технологиях, и прочих средств уменьшения риска перечень требований безопасности должен быть расширен.

Примечание — Настоящий стандарт не содержит требований к СБЗС системам, основанным на неэлектрических технологиях. В случае применения таких систем учитывают лишь обеспечиваемое ими снижение уровня риска.

7.5.4 В случаях, когда могут быть сделаны обоснованные допущения о рисках, вероятности опасностей, опасных событиях и их последствиях, и имеются результаты анализа, предусмотренного в подразделе 7.4, требования могут быть представлены в упрощенной форме, в соответствии с ГОСТ 34332.1 (приложения К, Л).

7.5.5 Для каждой проектной опасности должны быть определены функции безопасности, реализуемые Э/Э/ПЭ СБЗС системами и прочими средствами уменьшения риска, необходимые для обеспечения требуемой безопасности здания (сооружения). Должна быть определена спецификация требований к функциям безопасности и к их полноте безопасности.

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

Для каждой полной функции безопасности должны быть определены требования к целевой полноте безопасности, которая позволит обеспечить достижение приемлемого риска. Каждое требование может быть определено количественным и/или качественным методом. Его включают в полную спецификацию требований к полноте безопасности.

Требования к полноте безопасности системы могут быть определены в форме:

- необходимого снижения риска для достижения приемлемого риска, или
- допустимой частоты (интенсивности) опасных событий, удовлетворяющей приемлемому риску.

7.5.7 Если при оценке риска УО средняя частота опасных отказов отдельной функции системы управления УО оказалась ниже, чем 10^{-5} опасных отказов в час, то такую систему управления УО считают системой управления, связанной с безопасностью, которая должна удовлетворять требованиям настоящего стандарта.

Пример — Если для указанной системы управления УО средняя частота опасных отказов оказалась между значениями 10^{-6} и 10^{-5} в час, то эту систему рассматривают как систему, связанную с безопасностью, удовлетворяющую требованиям УПБ 1.

7.5.8 В случаях, когда отказы системы управления УО вызывают запросы к одной или нескольким Э/Э/ПЭ СБЗС системам и когда система управления УО не определена как СБ система, следует выполнять следующие требования:

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

а) на основании практического опыта работы системы управления УО в аналогичных условиях применении и при аналогичных уровнях сложности;

б) на основе достоверного анализа, осуществленного по официально признанной процедуре (например, установленной в национальных стандартах, сводах правил), либо

в) из промышленной базы данных по надежности оборудования этого вида;

- частота (интенсивность) опасных отказов, которая может потребоваться для систем управления УО, должна быть не ниже, чем 10^{-5} опасных отказов в час;
- при разработке перечня общих требований безопасности должны быть определены и приняты во внимание все обоснованно предсказуемые режимы опасных отказов системы управления УО;
- система управления УО должна быть независима и отделена от других СБЗС систем и прочих средств уменьшения риска.

7.5.9 Если требования 7.5.8 не могут быть выполнены, то систему управления УО следует рассматривать как систему, связанную с безопасностью. Уровень ее полноты безопасности должен быть выражен в величинах отказов по запросам в соответствии с пределами целевых отказов, установлен-

ными в 7.6.9 и 7.6.10. В этом случае требования настоящего стандарта, относящиеся к Э/Э/ПЭ СБЗС системам, должны быть применены к системам управления УО.

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

7.5.11 Полная спецификация требований к функции безопасности включает в себя перечень требований к функции безопасности (ее назначению) и перечень требований к полноте безопасности (см. 7.5.6).

7.6 Распределение требований безопасности

7.6.1 Функции безопасности, содержащиеся в спецификации полных требований к безопасности (требований к функциям безопасности и требований к полноте безопасности), и УПБ для каждой функции безопасности на этапе распределения требований безопасности (см. блок 5 на рисунке 1) должны быть распределены по назначенным Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска.

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

Примечания

1 Настоящий пункт применяют тогда, когда хотя бы одна из СБЗС систем является Э/Э/ПЭ системой.

2 СБЗС системы, основанные на неэлектрических технологиях, и прочие средства уменьшения риска принимают во внимание только тогда, когда распределение по Э/Э/ПЭ СБЗС системам не приводит к необходимому снижению риска иначе, как с использованием этих систем и средств.

3 В случае использования СБЗС систем, основанных на неэлектрических технологиях, на стадиях их ЖЦ учитывают лишь уровень снижения риска этими системами.

7.6.3 При распределении требований безопасности по назначенным Э/Э/ПЭ СБЗС системам и прочим 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.

7.6.4 Каждую функцию безопасности с относящимся к ней требованием к полноте безопасности, расширенном в соответствии с 7.5, распределяют по назначенным Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска (рисунок 2) таким образом, чтобы для этой функции безопасности было достигнуто необходимое снижение риска.

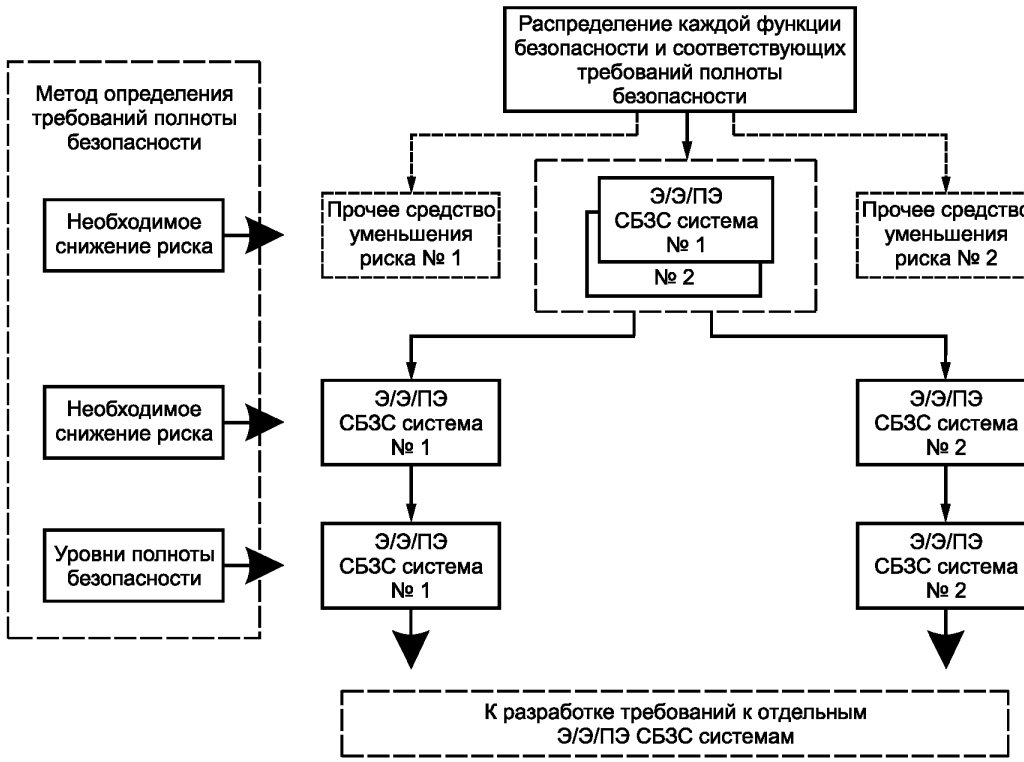


Рисунок 2 — Распределение функции безопасности по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска

7.6.5 Если обнаружено, что необходимое снижение риска не может быть достигнуто, то структуру системы изменяют, и распределение требований безопасности по системам и средствам проводят вновь в соответствии с ГОСТ 34332.1 (пункт 7.2.1 и рисунок 3).

Примечание — Итерационный процесс представлен также в [1] (пункт 6.1 и рисунок 2).

7.6.6 Распределение функций и требований безопасности по Э/Э/ПЭ СБЗС системам и прочим средствам уменьшения риска по 7.6.4 должно быть выполнено таким образом, чтобы все функции безопасности были распределены, и для каждой функции безопасности были выполнены требования к полноте безопасности.

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

- средней вероятностью отказов от выполнения ее назначенной функции по запросу (для режима работы с низкой частотой запросов) или
- средней частотой (интенсивностью) опасных отказов в час (для режима работы с высокой частотой запросов или с непрерывным запросом).

7.6.8 Распределение требований к полноте безопасности осуществляют с использованием комбинации вероятностей с применением количественных или качественных методов.

7.6.9 В ходе распределения функций безопасности учитывают вероятность отказов по общей причине.

7.6.10 Чтобы СБЗС системы и прочие средства уменьшения риска при распределении функций безопасности могли быть рассмотрены как независимые системы и средства, они должны:

- быть функционально различными, т. е. основанными на различных подходах для получения одних и тех же результатов;
- быть основанными 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 Э/Э/ПЭ СБЗС системы и прочие средства уменьшения риска.

7.6.11 Если не все требования 7.6.10 могут быть выполнены, то СБЗС системы и прочие средства уменьшения риска при распределении функции 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.

7.6.12 На завершающем этапе распределения требований к полноте безопасности для каждой функции безопасности, распределенной по Э/Э/ПЭ СБЗС системам, требования должны быть выражены в значениях целевых величин отказов в зависимости от УПБ в соответствии с таблицами 1 и 2.

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

УПБ	Средняя вероятность опасных отказов по запросу функции безопасности (PFD_{avg})
УПБ 4	Св. 10^{-5} до 10^{-4}
УПБ 3	Св. 10^{-4} до 10^{-3}
УПБ 2	Св. 10^{-3} до 10^{-2}
УПБ 1	Св. 10^{-2} до 10^{-1}

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

УПБ	Средняя частота (интенсивность) опасных отказов по запросу функции безопасности (*PFH*), [час$^{-1}$]
УПБ 4	Св. 10^{-9} до 10^{-8}
УПБ 3	Св. 10^{-8} до 10^{-7}
УПБ 2	Св. 10^{-7} до 10^{-6}
УПБ 1	Св. 10^{-6} до 10^{-5}

Примечание к таблицам 1 и 2 — 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
- средняя частота (интенсивность) опасных отказов в час (для режима работы с высокой частотой запросов или с постоянным запросом).

7.6.13 Для Э/Э/ПЭ СБЗС систем, работающих в режиме с высокой частотой запросов или с непрерывным запросом, для которых во время выполнения функции(ий) безопасности восстановление невозможно, требуемый УПБ 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 функции(ий) для получения требуемой частоты (интенсивности) отказов в час; затем используют таблицу 2 для получения требуемого УПБ.

7.6.14 Для Э/Э/ПЭ СБЗС системы, которая выполняет функции безопасности различного УПБ, те части АС и ПО, которые недостаточно независимы при реализации функций безопасности, должны рассматриваться как выполняющие функции безопасности с наивысшим УПБ. 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 УПБ.

7.6.15 Структура СБЗС системы, состоящей из одиночной Э/Э/ПЭ системы с УПБ 4, может быть допущена к применению только в случае, если будет выполняться первое перечисление, либо одновременно второе и третье перечисления, приведенные ниже:

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

- имеется обширный опыт эксплуатации составляющих (модулей), используемых как часть Э/Э/ПЭ СБЗС системы, полученный в условиях подобного окружения и в системе сопоставимого уровня сложности;

- имеются достоверные данные по отказам аппаратуры, состоящей из модулей, используемых как часть Э/Э/ПЭ СБЗС системы, соответствующие требуемым целевым значениям полноты безопасности.

7.6.16 Указанные данные по отказам следует относить к планируемому окружению, применению и сложности.

7.6.17 Ни одна одиночная Э/Э/ПЭ 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 Э/Э/ПЭ 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 непрерывным запросом, нижний предел должен быть установлен как частота (интенсивность) 10^{-9} опасных отказов в час.

7.6.18 Информация и результаты распределения требований безопасности, полученные в 7.6.2—7.6.17, а также все сделанные допущения и обоснования должны быть документированы.

7.7 Разработка проектной документации на системы, связанные с безопасностью

7.7.1 Разработку раздела, подраздела или пункта проектной документации с мероприятиями по 5.2.4 осуществляют в соответствии с требованиями задания на проектирование, технических условий или специальных технических условий (при их наличии).

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 опасности, сложности и ответственности.

7.7.3 Разработку проектной документации на СБЗС системы осуществляют в соответствии с процедурами, предусмотренными принятой в проектной организации системой менеджмента качества, не противоречащей требованиям ГОСТ ISO 9001.

7.7.4 При разработке проектной документации на Э/Э/ПЭ СБЗС системы применяют итерационный процесс анализа опасностей и рисков, общей оценки риска и снижения риска в соответствии с ГОСТ 34332.1 (подраздел 7.2) и [5] для достижения приемлемого риска.

7.7.5 В состав проектной документации включают:

- перечень и состав всех Э/Э/ПЭ СБЗС систем и прочих средств уменьшения риска, предусмотренных в 7.6, включая наименование и версию ПО, используемого для каждой из Э/Э/ПЭ СБЗС систем или подсистем;

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

- структурную и/или функциональную схему КСБ;

- схемы соединений Э/Э/ПЭ СБЗС систем при объединении их в КСБ;

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

- наименование и краткое описание прикладного ПО, применяемого для интеграции Э/Э/ПЭ СБЗС систем в КСБ здания (сооружения), включая описание способов достижения информационной совместимости систем;

- структурные и/или функциональные схемы взаимодействия с оборудованием внешних служб (по чрезвычайным ситуациям, экстренной медицинской помощи, правоохранительных органов, внешних диспетчерских служб) и внутренних диспетчерских служб, а также схемы соединений с этим оборудованием;

- описание алгоритмов взаимодействия Э/Э/ПЭ СБЗС систем и подсистем в составе КСБ объекта:

  а) при подготовке к пуску, включая установку и пусконаладку,

  б) при нормальной эксплуатации в штатных режимах,

в) при отключении,

г) в период проведения регламентных работ,

д) в предаварийных ситуациях,

е) при аварийных, кризисных и чрезвычайных ситуациях,

ж) 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 (по чрезвычайным ситуациям, экстренной медицинской помощи, правоохранительными органами, внешними диспетчерскими службами) и внутренними диспетчерскими службами;
- требования к размещению оборудования и периферийных средств контроля и управления Э/Э/ПЭ СБЗС систем; при этом особое внимание должно быть уделено:

а) контролю жизненно важных помещений, зон и критически важных точек объекта,

б) контролю путей эвакуации людей,

в) одновременному применению в ответственных зонах элементов контроля и управления различных Э/Э/ПЭ 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 Э/Э/ПЭ СБЗС систем.

7.7.6 В случае применения СБЗС систем, основанных на неэлектрических технологиях, и прочих средств уменьшения риска, требования к ним и их характеристики должны быть включены в комплект проектной документации.

7.7.7 Документацию следует формировать в соответствии с 5.2 и оформлять с учетом информации, приведенной в приложении А.

7.7.8 По завершении разработки раздела, подраздела или пункта проекта должен быть проведен аудит документации, перечисленной в 7.7.2—7.7.6, с привлечением независимого эксперта (экспертов), независимого подразделения или независимой организации.

7.7.9 Документация раздела, подраздела или пункта проекта в соответствии с 5.2.4 и 7.7.1 должна быть согласована с заинтересованными подразделениями и/или организациями (указанными в задании на проектирование, технических условиях или специальных технических условиях (при их наличии) и утверждена в установленном порядке.

7.7.10 После утверждения раздела, подраздела или пункта проекта по 5.2.4 и 7.7.1 обеспечивают доступность ключевой информации лицам, ответственным за комплексное обеспечение безопасности здания (сооружения).

7.7.11 Документация подраздела или пункта по 5.2.4 и 7.7.1, включая все последующие внесенные по установленным процедурам изменения и дополнения, должна быть сохранена в хронологическом порядке вплоть до полного завершения ЖЦ Э/Э/ПЭ СБЗС систем, КСБ и объекта.

7.8 Разработка рабочей документации

7.8.1 Для обеспечения должного выполнения действий по реализации последующих стадий ЖЦ Э/Э/ПЭ СБЗС систем и КСБ, а также ЖЦ здания (сооружения) должна быть разработана соответствующая рабочая документация на эти системы (см. блок 7 на рисунке 1).

7.8.2 При разработке рабочей документации на Э/Э/ПЭ СБЗС системы и КСБ должны быть учтены архитектурные, функционально-технологические, объемно-планировочные, конструктивные и инженерные решения утвержденного в установленном порядке проекта на здание (сооружение).

7.8.3 В период разработки рабочей документации на Э/Э/ПЭ СБЗС системы и КСБ для обеспечения реализации последующих стадий их ЖЦ разрабатывают следующие документы:

- рабочие чертежи главного центра управления службы безопасности здания (сооружения) — центра управления кризисными ситуациями, периферийных центров и резервного пункта управления (при их наличии);
- рабочие чертежи на монтаж оборудования и периферийных устройств Э/Э/ПЭ СБЗС систем;
- рабочие чертежи (строительные задания) на прокладку кабелей Э/Э/ПЭ СБЗС систем;

- кабельные журналы;
- инструкции по установке (монтажу), пуску, регулированию оборудования и периферийных средств Э/Э/ПЭ СБЗС систем;
- ПО для Э/Э/ПЭ СБЗС систем и руководства к ним;
- тестовые программы для контроля Э/Э/ПЭ СБЗС систем и руководства к ним;
- базовые методы испытаний и оценки соответствия Э/Э/ПЭ СБЗС систем, их АС и ПО;
- инструкцию по интеграции Э/Э/ПЭ СБЗС систем в КСБ, пусконаладке системы;
- тестовые программы для контроля КСБ и руководства к ним;
- базовые методы испытаний и оценки соответствия КСБ, АС и ПО;
- руководство по эксплуатации Э/Э/ПЭ СБЗС систем;
- руководство по эксплуатации КСБ;
- формуляры (журналы) на Э/Э/ПЭ СБЗС-системы;
- формуляр (журнал) на КСБ;
- каталог (список) Э/Э/ПЭ СБЗС систем и их составляющих;
- инструкции по техническому обслуживанию и ремонту Э/Э/ПЭ СБЗС систем и их составляющих.

Примечание — Порядок технического обслуживания и ремонта Э/Э/ПЭ СБЗС может быть установлен в отдельном стандарте;

- нормы расхода запасных частей (если они предусмотрены);
- нормы расхода материалов (если они предусмотрены);
- журнал комплекта запасных частей, инструментов, принадлежностей и материалов (если они предусмотрены);
- эксплуатационные специальные инструкции, при необходимости;
- инструкция по порядку вывода из эксплуатации и утилизации Э/Э/ПЭ СБЗС систем.

7.8.4 До реализации и ввода в действие Э/Э/ПЭ 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

7.9.1 Для обеспечения достижения требуемой функциональной безопасности Э/Э/ПЭ СБЗС систем до установки их оборудования в здании (сооружении) должны быть разработаны в контролируемой форме (см. блок 8 на рисунке 1) планы:

- реализации, установки (монтажа) Э/Э/ПЭ СБЗС систем;
- ввода в действие Э/Э/ПЭ СБЗС систем;
- интеграции Э/Э/ПЭ СБЗС систем в единую систему комплексного обеспечения безопасности здания (сооружения).

7.9.2 Лицами, ответственными за реализацию систем на объекте, должен быть разработан план установки (монтажа) Э/Э/ПЭ СБЗС систем, определяющий:

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

7.9.3 В плане ввода в действие Э/Э/ПЭ СБЗС систем должны быть определены:

- график ввода в действие;
- методика и процедуры для оценки результатов испытаний, расчетов, особенно отказов;
- критерии «соответствия»/«не соответствия» требованиям, а также возможности обхода систем.

7.10 Планирование оценки и подтверждения соответствия

7.10.1 При разработке плана подтверждения соответствия (см. блок 9 на рисунке 1) должны быть приняты во внимание результаты действий по планированию подтверждения функциональной безопасности АС и ПО Э/Э/ПЭ СБЗС систем; при этом следует удостовериться в том, что взаимовлияние между

всеми принятыми мерами по снижению риска рассмотрено, и все действия, предусмотренные в 7.5, выполнены.

7.10.2 Для КСБ особо опасных, технически сложных и уникальных объектов, а также объектов повышенного уровня ответственности, имеющих важное экономическое и социальное значение, 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 здания (сооружения).

7.10.3 Информация по 7.10.1 и 7.10.2 должна быть документирована и сохранена.

7.11 Планирование эксплуатации и технического обслуживания систем

7.11.1 Лицами, ответственными за ввод в эксплуатацию здания (сооружения), должен быть разработан (см. блок 10 на рисунке 1) план эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС систем, в том числе КСБ, включая периодические контрольные проверки, для поддержания требуемой функциональной безопасности в период эксплуатации и технического обслуживания систем.

7.11.2 В план включают:

- типовые действия, которые необходимо выполнять для поддержания требуемой функциональной безопасности Э/Э/ПЭ СБЗС систем, в том числе КСБ;
- 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 Э/Э/ПЭ СБЗС системам или снижения тяжести последствий опасных событий, в том числе:

а) ограничения УО при эксплуатации во время неисправности или отказа Э/Э/ПЭ СБЗС систем;

б) ограничения УО при эксплуатации в период технического обслуживания Э/Э/ПЭ СБЗС систем;

в) действия, когда ограничения УО в период эксплуатации могут быть устранены;

г) процедуры для возвращения к нормальной эксплуатации систем;

д) процедуры, подтверждающие, что нормальная эксплуатация систем достигнута;

е) ограничения, из-за которых функции Э/Э/ПЭ СБЗС системы могут быть не использованы для пуска, специального режима работы или тестирования;

ж) процедуры, которые должны следовать до, во время и после обхода Э/Э/ПЭ СБЗС систем, включая допуск к рабочим процедурам и уровни полномочий;

- информацию о результатах аудита функциональной безопасности и тестирования, подлежащую сохранению;
- информацию об опасных ситуациях и всех ситуациях, которые потенциально приводят к опасному событию, подлежащую сохранению;
- масштаб действий по техническому обслуживанию, контрольным испытаниям и их периодичности;
- действия, которые должны быть предприняты в случае появления опасных событий;
- 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 Э/Э/ПЭ СБЗС систем и КСБ здания (сооружения), а также квалификации персонала, осуществляющего техническое обслуживание этих систем.

7.11.4 Действия по техническому обслуживанию, которые осуществляют для обнаружения скрытых неисправностей, следует выполнять на основе мониторинга и систематического анализа.

7.11.5 План по техническому обслуживанию Э/Э/ПЭ СБЗС систем должен быть согласован с лицами, ответственными за будущую эксплуатацию и техническое обслуживание СБЗС систем и прочих средств уменьшения риска, а также систем, не связанных с безопасностью, которые потенциально могут иметь запрос к Э/Э/ПЭ СБЗС системам (если эти лица известны).

7.12 Реализация Э/Э/ПЭ СБЗС систем

7.12.1 При реализации (установке, монтаже, пусконаладке) Э/Э/ПЭ СБЗС систем в здании (сооружении) (см. блок 11 на рисунке 1) следует предусматривать подготовку систем в соответствии с перечнем требований к Э/Э/ПЭ СБЗС системам, включая перечни требований к АС и ПО.

7.12.2 До установки (монтажа) АС и ПО Э/Э/ПЭ 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 быть выполнены в соответствии с документацией по установке (монтажу). Очередность и порядок выполнения работ должны соответствовать плану по установке (монтажу) Э/Э/ПЭ СБЗС систем.

7.12.4 В документацию по установке (монтажу) Э/Э/ПЭ СБЗС систем включают:

- документацию по действиям по установке, регулировке и пусконаладке Э/Э/ПЭ СБЗС систем и их составляющих;
- документацию по интеграции систем в КСБ и вводу в действие;
- документацию по разрешению отказов и несовместимости.

7.13 Реализация СБЗС систем, основанных на неэлектрических технологиях

До установки в зданиях (сооружениях) СБЗС систем, основанных на неэлектрических технологиях (см. блок 12 на рисунке 1), должно быть подтверждено их соответствие спецификации, требованиям назначения и требованиям безопасности, установленным в проектной документации.

7.14 Реализация прочих средств уменьшения риска

До реализации (установки) в здании (сооружении) и на прилегающей территории прочих средств уменьшения риска (см. блок 13 на рисунке 1) должно быть подтверждено их соответствие требованиям назначения и требованиям безопасности, установленным в проектной документации.

7.15 Оценка и подтверждение соответствия

7.15.1 Лицами, ответственными за ввод здания (сооружения) в эксплуатацию, должно быть организовано проведение оценки и подтверждения соответствия установленных на объекте Э/Э/ПЭ СБЗС систем и КСБ (см. блок 14 на рисунке 1) полным требованиям функциональной безопасности согласно плану оценки и подтверждения соответствия Э/Э/ПЭ СБЗС систем и КСБ предусмотренным требованиям (см. подраздел 7.10).

7.15.2 В документацию, составляемую в период подтверждения соответствия, включают:

- сведения о действиях по оценке и подтверждению соответствия, в хронологическом порядке;
- используемую версию спецификации полных требований к функциональной безопасности;
- перечень функций безопасности, соответствие которых оценивают и подтверждают с помощью испытаний (тестирования) или анализа;
- перечень средств испытаний, тестовых программ, измерительных приборов и данные об их аттестации и поверке;
- результаты действий по оценке и подтверждению соответствия;
- подробную идентификацию пункта испытаний, применяемых процедур и условий испытаний;
- сведения о различии между ожидаемыми и полученными фактическими результатами.

7.15.3 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 возврату к более раннему этапу подтверждения соответствия.

7.16 Эксплуатация, техническое обслуживание, ремонт, периодический контроль

7.16.1 Эксплуатацию, техническое обслуживание, текущий ремонт и периодический контроль Э/Э/ПЭ СБЗС систем, включая КСБ (см. блок 15 на рисунке 1), осуществляют таким образом, чтобы в период эксплуатации систем поддерживались заданные требования к функциональной безопасности.

7.16.2 Должно быть обеспечено выполнение:

- плана эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС систем, включая КСБ (см. подраздел 7.11);
- процедур эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС систем;
- процедур эксплуатации и поддержки ПО Э/Э/ПЭ СБЗС систем, включая КСБ;
- процедур периодических проверок (испытаний, тестирования) Э/Э/ПЭ СБЗС систем, включая КСБ, в том числе органами государственного или негосударственного контроля (надзора).

7.16.3 При выполнении положений по 7.16.2 обеспечивают:

- следование графику технического обслуживания;

- исполнение процедур;
- ведение документации;
- периодическое осуществление аудита (проверки) функциональной безопасности;
- документирование выполненных модификаций Э/Э/ПЭ СБЗС систем.

Типичная последовательность действий в период эксплуатации и текущего ремонта систем представлена на рисунке 3. Типичная последовательность действий по управлению эксплуатацией и техническим обслуживанием систем представлена на рисунке 4.

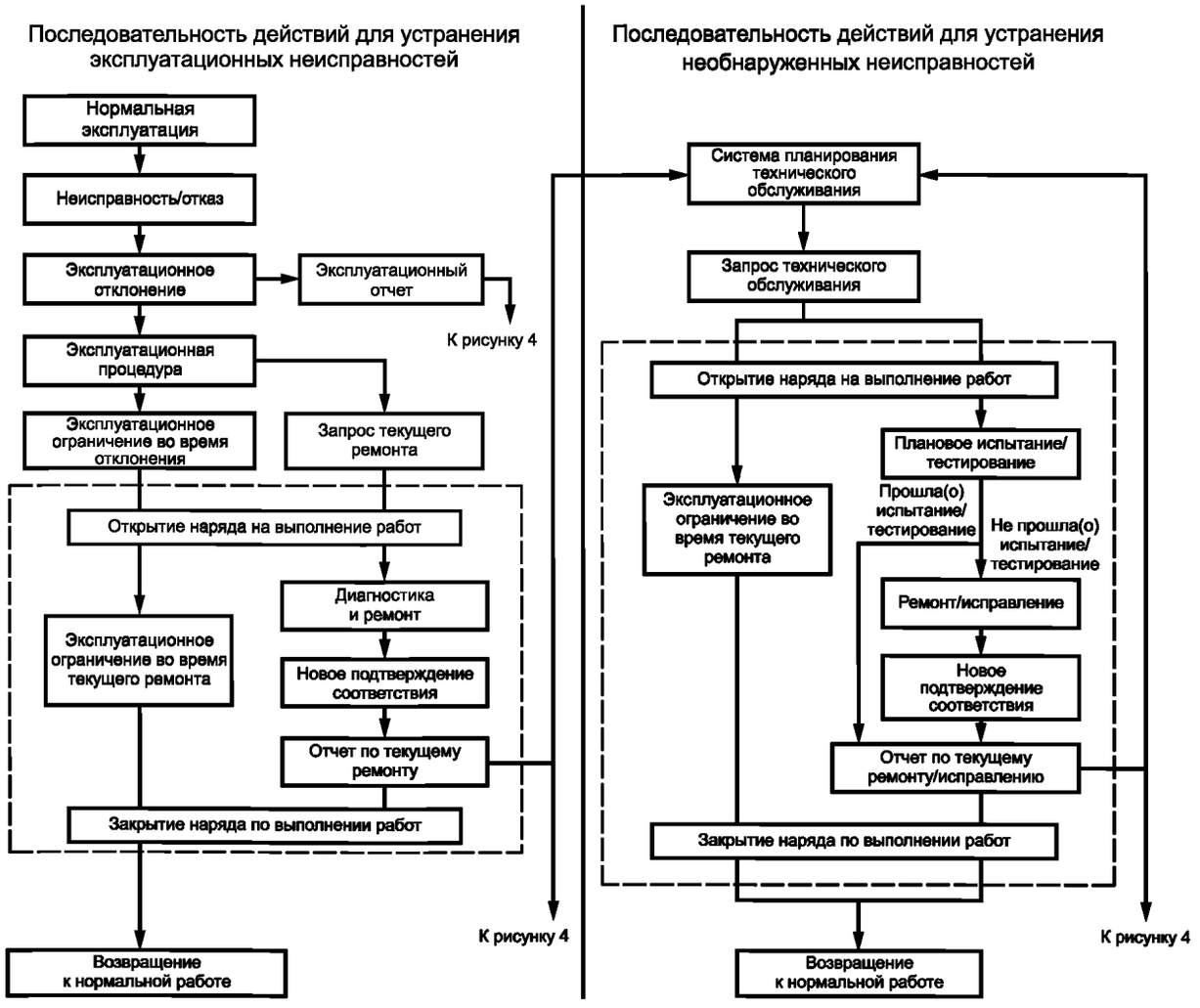


Рисунок 3 — Типичная последовательность действий в период эксплуатации и текущего ремонта систем

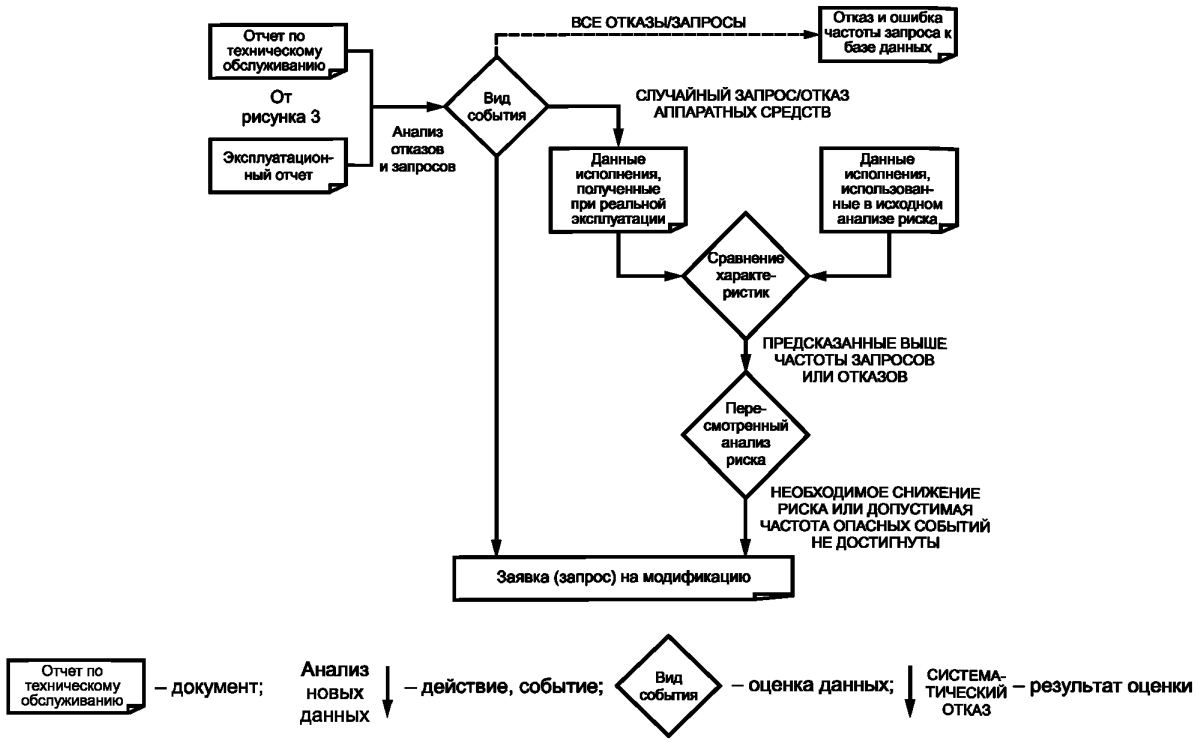


Рисунок 4 — Типичная последовательность действий по управлению эксплуатацией и техническим обслуживанием систем

7.16.4 В документацию, создаваемую в хронологическом порядке при эксплуатации, ремонте и техническом обслуживании Э/Э/ПЭ СБЗС систем, включают:

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

7.16.5 Документацию следует сохранять в течение всего периода эксплуатации систем, вплоть до вывода их из эксплуатации и утилизации.

7.17 Видоизменение и модификация

7.17.1 Видоизменение и модификацию Э/Э/ПЭ СБЗС систем и КСБ (см. блок 16 на рисунке 1) следует осуществлять 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 (модификации) Э/Э/ПЭ СБЗС систем и КСБ эти процедуры должны быть запланированы в соответствии с 6.2.

Типичная модель процедур видоизменения (модификации) систем представлена на рисунке 5.

7.17.3 Этап видоизменения или модификации может быть инициирован только на основании авторизованной заявки (см. рисунок 5), оформленной в соответствии с процедурами управления функциональной безопасностью, установленными в разделе 6. В заявку включают следующую информацию:

- заданные проектные опасности, которые могут иметь место;
- предлагаемые изменения АС и/или ПО;
- обоснование для изменений.

Основанием для заявки на видоизменение и модификацию могут быть:

- 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 применения;
- 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 или негосударственного контроля (надзора), установившие несоответствие требованиям безопасности и выдавшие соответствующее предписание органов контроля (надзора) по его устранению.

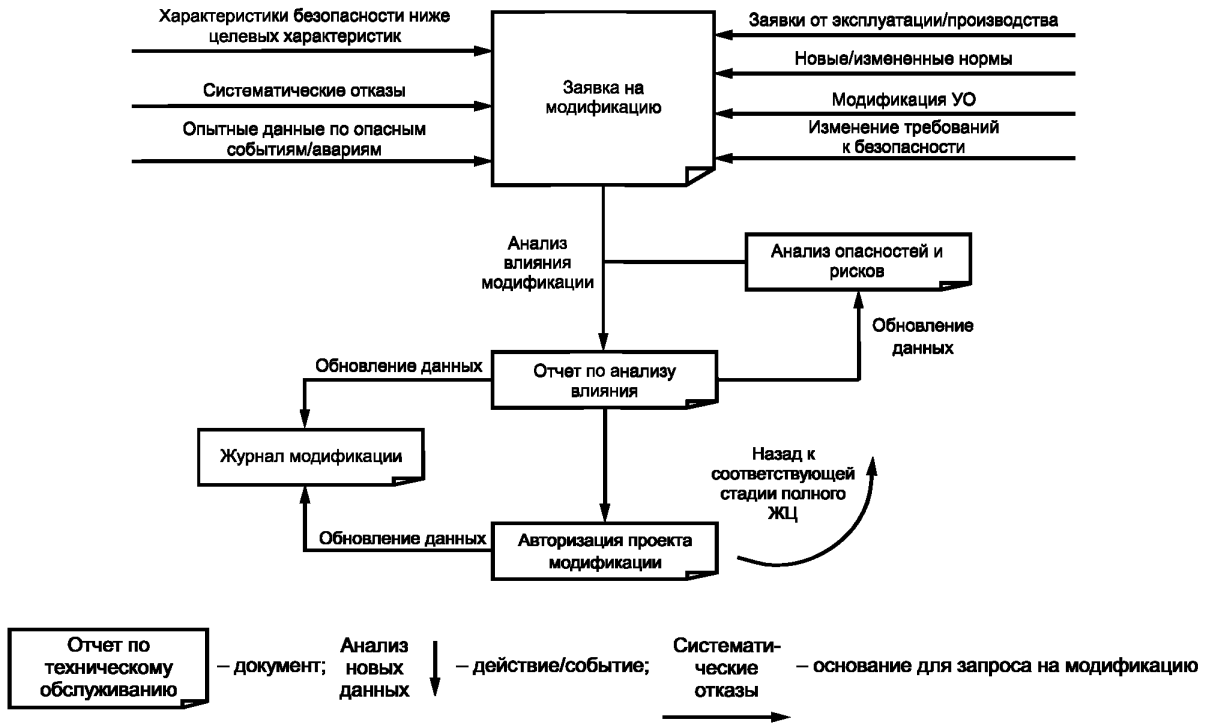


Рисунок 5 — Типичная модель процедур видоизменения (модификации) систем

7.17.4 До осуществления видоизменения (модификации) Э/Э/ПЭ СБЗС систем и КСБ должен быть проведен анализ влияния, включающий в себя оценку влияния предложенного видоизменения (модификации) либо действий по видоизменению (модификации) на функциональную безопасность Э/Э/ПЭ СБЗС систем и КСБ.

7.17.5 В оценку влияния включают анализ опасностей и рисков, которые могут возникнуть на последующих стадиях ЖЦ Э/Э/ПЭ СБЗС систем и КСБ, их АС или ПО. При оценке влияния следует также учитывать влияние других видоизменений и модификаций или действий по видоизменениям (модификациям) и следует учитывать функциональную безопасность, имеющую место как в период осуществления видоизменений или модификаций, так и после их проведения или действий по видоизменениям или модификациям.

7.17.6 Результаты, полученные по 7.17.5, должны быть документированы. Разрешение на осуществление требуемого видоизменения (модификации) либо действий по видоизменению (модификации) определяют с учетом результатов анализа влияния.

7.17.7 Все видоизменения (модификации), которые оказывают влияние на функциональную безопасность любой Э/Э/ПЭ СБЗС системы, включая КСБ, начинают с возврата к соответствующей стадии ЖЦ системы, ЖЦ АС или ПО. Все последующие стадии должны быть осуществлены в соответствии с процедурами, установленными для этих стадий, и требованиями настоящего стандарта.

7.17.8 В случае отличия реальных оцененных или измеренных УПБ от заданных для Э/Э/ПЭ СБЗС систем УПБ следует провести полный анализ опасностей и рисков.

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

7.17.10 Должна быть создана и сохранена в хронологическом порядке документация, содержащая детали всех видоизменений (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 видоизменения (модификации) и действия по видоизменениям (модификациям).

7.18 Вывод из эксплуатации и утилизация

7.18.1 Вывод из эксплуатации Э/Э/ПЭ СБЗС систем (см. блок 17 на рисунке 1) следует осуществлять таким образом, чтобы безопасность объекта не снижалась из-за обстоятельств, возникающих во время вывода из эксплуатации этих систем, УО, систем управления УО и после их завершения.

7.18.2 Лицами, ответственными за безопасность здания (сооружения) в этот период времени, должны быть приняты дополнительные защитные меры, компенсирующие повышение риска, обусловленного выводом из эксплуатации данной Э/Э/ПЭ СБЗС системы.

7.18.3 Перед выводом из эксплуатации одной из Э/Э/ПЭ 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 Э/Э/ПЭ СБЗС системы, УО и системы управления УО.

При анализе влияния должны быть также учтены смежные УО и их влияние на Э/Э/ПЭ СБЗС системы. Оценка влияния должна включать в себя анализ опасностей и рисков, которые могут возникнуть на последующих стадиях полного ЖЦ смежных Э/Э/ПЭ СБЗС систем или ЖЦ АС либо ПО.

7.18.4 Утилизацию Э/Э/ПЭ СБЗС систем и УО осуществляют в соответствии с требованиями экологической безопасности.

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

7.18.6 Стадии вывода из эксплуатации или утилизации Э/Э/ПЭ СБЗС систем должны быть инициированы исключительно на основании санкционированного запроса или заявки в соответствии с процедурами по управлению функциональной безопасностью, определенными в разделе 6.

7.18.7 Разрешение на осуществление требуемого вывода Э/Э/ПЭ СБЗС систем из эксплуатации следует выдавать с учетом результатов анализа влияния.

7.18.8 До вывода систем из эксплуатации должен быть подготовлен план, который должен содержать процедуры по отключению и демонтажу Э/Э/ПЭ СБЗС систем.

7.18.9 Если какие-либо действия по выводу из эксплуатации оказывают влияние на функциональную безопасность любой другой Э/Э/ПЭ СБЗС системы, эти действия следует начинать с возврата к соответствующей стадии полного ЖЦ такой системы, ЖЦ АС или ПО. Затем должны быть осуществлены все последующие стадии в соответствии с процедурами, определенными в настоящем стандарте для заданных УПБ для Э/Э/ПЭ СБЗС систем.

Если стадия вывода из эксплуатации Э/Э/ПЭ 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.

7.18.10 Следует формировать и сохранять в хронологическом порядке документацию, содержащую документальные подробности действий по выводу из эксплуатации Э/Э/ПЭ СБЗС систем, и ссылки на план, используемый для действий по выводу из эксплуатации, а также ссылки на анализ влияния.

7.19 Верификация систем

7.19.1 Для каждой стадии ЖЦ Э/Э/ПЭ СБЗС систем должна быть проведена верификация с представлением свидетельств, полученных с помощью проверки, анализа, расчетов и/или испытаний того, что для каждой стадии полного ЖЦ Э/Э/ПЭ СБЗС систем результаты соответствуют всем целям и требованиям, определенным для этой стадии.

7.19.2 Верификацию следует осуществлять 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 приведены ссылки на них.

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

- степень опасности, технической сложности, уровень ответственности объекта, в котором применены Э/Э/ПЭ СБЗС системы;
- состав и число систем в проекте;
- степень сложности Э/Э/ПЭ СБЗС систем;
- степень новизны разработки;
- степень новизны технологии.

Примечание — Чем более сложный и объемный проект, чем выше степень новизны разработки и технологии Э/Э/ПЭ 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 завершена.

8 Оценка функциональной безопасности

8.1 Цель

Целью требований настоящего раздела является определение действий, необходимых для изучения и вынесения решения по адекватности функциональной безопасности, достигнутой Э/Э/ПЭ СБЗС системой(ами) или составляющими (например, подсистемами или модулями) на основе соблюдения соответствующих положений настоящего стандарта.

8.2 Требования

8.2.1 Для выполнения одной или более оценок функциональной безопасности необходимо назначить одно лицо или большее число лиц для вынесения суждений об адекватности:

- функциональной безопасности, достигаемой Э/Э/ПЭ СБЗС системой в конкретной окружающей ее среде, соответствующим положениям настоящего стандарта;
- выполнения соответствующих положений настоящего стандарта в отношении составляющих (подсистем или модулей).

Эти лица должны быть в полной мере информированы о возложенной на них ответственности.

8.2.2 Лица, выполняющие оценку функциональной безопасности, должны иметь доступ ко всем лицам, выполняющим любые действия на всех стадиях ЖЦ Э/Э/ПЭ СБЗС систем, их АС или ПО, а также ко всей информации и системам (включая АС и ПО).

Примечание — Поскольку лица, которые ранее участвовали в работах на различных стадиях ЖЦ системы безопасности, не всегда доступны, то ответственность должна быть возложена на лиц, имеющих в период осуществления оценки функциональной безопасности соответствующие функции.

8.2.3 Оценку функциональной безопасности следует осуществлять на всех стадиях ЖЦ Э/Э/ПЭ СБЗС системы, ее АС и ПО, а также применять к документации при верификации и управлении функциональной безопасностью.

8.2.4 Лица, осуществляющие оценку функциональной безопасности, должны рассмотреть все выполненные действия, а также все результаты, полученные в течение каждой стадии ЖЦ Э/Э/ПЭ СБЗС системы, ЖЦ АС и ПО и дать заключение о том, в какой степени достигнуты цели и выполнены требования настоящего стандарта.

8.2.5 Все соответствующие заявления (декларации) о соответствии, предоставленные поставщиками и другими сторонами, ответственными за достижение функциональной безопасности, должны быть включены в оценку функциональной безопасности.

Примечание — Такие заявления (декларации) могут быть предоставлены для действующей системы или для вклада в функциональную безопасность на каждой стадии ЖЦ Э/Э/ПЭ СБЗС системы, АС и ПО.

8.2.6 Оценку функциональной безопасности предпочтительно выполнять после каждой стадии ЖЦ всей Э/Э/ПЭ СБЗС системы, АС и ПО.

Допускается выполнять оценку функциональной безопасности после нескольких стадий при условии выполнения основного требования: оценку функциональной безопасности следует осуществлять до возникновения выявленных опасностей.

8.2.7 В оценку функциональной безопасности включают оценку доказательств того, что был проведен (полностью или частично) аудит функциональной безопасности в соответствии с областью применения.

8.2.8 При оценке функциональной безопасности необходимо учитывать, как минимум, следующее:

- работы, выполненные со времени предыдущей оценки функциональной безопасности;
- планы или стратегию реализации последующих оценок функциональной безопасности для ЖЦ полной Э/Э/ПЭ СБЗС системы, ЖЦ АС и ПО;
- рекомендации предыдущих оценок функциональной безопасности и объем внесенных изменений.

8.2.9 Каждая оценка функциональной безопасности должна быть спланирована. В плане должна быть определена вся информация, необходимая для проведения эффективной оценки, включая:

- область применения оценки функциональной безопасности;
- вовлеченные организации;
- требуемые ресурсы;
- лиц, осуществляющих оценку функциональной безопасности;
- уровень независимости лиц (подразделений, организаций), выполняющих оценку функциональной безопасности;
- компетентность всех лиц, выполняющих оценку функциональной безопасности;
- выходные материалы при каждой оценке функциональной безопасности;
- как оценка функциональной безопасности соотносится и должна быть интегрирована с другими оценками функциональной безопасности в соответствующих случаях (см. 6.2.1).

Примечания

1 При установлении области применения оценки функциональной безопасности необходимо определить документы, используемые в качестве входных материалов для каждого действия, связанного с оценкой функциональной безопасности, и статус этих документов.

2 План может быть сформирован либо ответственными за оценку функциональной безопасности, либо ответственными за управление функциональной безопасностью, или его формирование может быть разделено между ними.

8.2.10 Перед выполнением оценки функциональной безопасности ее план должен быть утвержден теми, кто будет выполнять эту оценку, и теми, кто несет ответственность за управление функциональной безопасностью.

8.2.11 В заключении об оценке функциональной безопасности лица, выполняющие оценку, должны документально оформить в соответствии с планами оценки и их полномочиями:

- выполненные действия;
- полученные результаты;
- выводы;
- суждение об адекватности функциональной безопасности требованиям настоящего стандарта;
- рекомендации, вытекающие из оценки, в том числе рекомендации по принятию, условному принятию или отклонению.

8.2.12 Лицам, ответственным за любые действия на стадиях ЖЦ всей системы безопасности, Э/Э/ПЭ СБЗС системы, АС или ПО (включая проектировщиков и экспертов по Э/Э/ПЭ СБЗС системам, а также интеграторов Э/Э/ПЭ СБЗС систем) должна быть обеспечена доступность к соответствующим результатам оценки функциональной безопасности поставляемых составляющих.

Примечание — Поставляемая составляющая — это любое комплектующее техническое средство (например, изделие или система промышленного производства, аппаратный или программный модуль), включаемое в состав Э/Э/ПЭ СБЗС системы.

8.2.13 Для облегчения повторного использования результатов оценки ранее использованной поставляемой составляющей для более крупной системы в результат оценки функциональной безопасности включают следующую информацию:

- точное определение поставляемой составляющей, включая версии АС и ПО.

Примечание — Если поставляемая составляющая рассматривается как часть более крупной системы или как семейство оборудования, то точное определение этой системы или семейства оборудования должно быть документально оформлено;

- условия, предполагаемые в ходе оценки (например, условия использования Э/Э/ПЭ СБЗС системы);
- ссылку на документально оформленное доказательство, на котором основана заключительная оценка;
- процедуры, методы и средства, использованные для оценки стойкости к систематическим отказам вместе с обоснованием их эффективности;
- процедуры, методы и средства, использованные для оценки полноты безопасности АС вместе с обоснованием используемого подхода и качества данных (например, интенсивность отказов или сведения об источниках данных);
- оценку результатов, полученных в соответствии с требованиями настоящего стандарта, и спецификации характеристик системы для применяемой составляющей в соответствующем руководстве по безопасности;
- принятые отклонения от требований, установленных в настоящем стандарте, с соответствующими разъяснениями и/или ссылками на доказательства, содержащиеся в документации.

8.2.14 Лица, осуществляющие оценку функциональной безопасности, должны обладать компетентностью, достаточной для осуществления мероприятий, которые выполняются в соответствии с 6.2.13—6.2.15.

8.2.15 Минимальный уровень независимости лиц, подразделений, организаций, выполняющих оценку функциональной безопасности, должен соответствовать тому уровню, который указан в таблицах 3 и 4.

В таблице 3 приведены требования к минимальному уровню независимости лиц, подразделений, организаций, осуществляющих оценку функциональной безопасности (блоки 1—10 и 14—18 ЖЦ Э/Э/ПЭ СБЗС систем) в зависимости от последствий опасного события.

В таблице 4 приведены требования к минимальному уровню независимости лиц, подразделений, организаций, осуществляющих оценку функциональной безопасности (блок 11 ЖЦ Э/Э/ПЭ СБЗС систем) в зависимости от целевого УПБ.

Таблица 3 — Минимальный уровень независимости лиц, подразделений, организаций, осуществляющих оценку функциональной безопасности (блоки 1—10 и 4—18 ЖЦ Э/Э/ПЭ СБЗС систем) в зависимости от последствий опасного события

Минимальный уровень независимости	Последствия опасных событий (см. 8.2.17)			
	A	*B*	*C*	*D*
Независимое лицо	*X*	*X*1	*Y*	*Y*
Независимое подразделение	—	*X*2	*X*1	*Y*
Независимая организация	—	—	*X*2	*X*

Примечания

1 Подробности по независимости в настоящей таблице, см. 8.2.15, 8.2.16 и 8.2.17.

2 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* — гибель нескольких человек; последствие *D* — гибель очень большого числа людей, см. также ГОСТ 34332.1 (приложение Б).

Таблица 4 — Минимальный уровень независимости лиц, подразделений, организаций, осуществляющих оценку функциональной безопасности (блок 11 ЖЦ Э/Э/ПЭ СБЗС систем) в зависимости от целевого УПБ.

Минимальный уровень независимости	УПБ /систематическая вероятность			
	1	2	3	4
Независимое лицо	*X*	*X*1	*Y*	*Y*
Независимое подразделение	—	*X*2	*X*1	*Y*
Независимая организация	—	—	*X*2	*X*

Примечания

1 Подробности по независимости в настоящей таблице, см. 8.2.15, 8.2.16 и 8.2.17.

2 В межгосударственных стандартах для других областей применения Э/Э/ПЭ СБЗС систем могут быть установлены отличные от указанных в таблицах 3 и 4 уровни независимости.

Обозначения в таблицах 3 и 4 следует интерпретировать следующим образом:

- *X* — уровень независимости, определенный в качестве минимального для указанных последствий (см. таблицу 3) или УПБ/стойкости к систематическим отказам (см. таблицу 4). Если принят более низкий уровень независимости, то этому должно быть приведено подробное обоснование;
- *X*1 и *X*2 — см. 8.2.16;
- *Y* — уровень независимости, определенный как недостаточный для указанных последствий (см. таблицу 3) или УПБ/стойкости к систематическим отказам (см. таблицу 4).

8.2.16 В контексте таблиц 3 и 4 в качестве основы для определения уровня независимости следует использовать только *X*, *X*1, *X*2 и *Y*. Если выбраны *X*1 или *X*2, то применяют либо *X*1, либо *X*2 (но не оба вместе) в зависимости от ряда факторов, характерных для области применения. Обоснование выбора *X*1 или *X*2 должно быть подробным. Факторы, которые делают *X*2 более предпочтительным, чем *X*1, следующие:

- недостаток опыта в работе со схожими проектами;
- более высокая степень сложности Э/Э/ПЭ СБЗС системы;
- более высокая степень новизны разработки;
- более высокая степень новизны технологии.

Примечания

1 В зависимости от организационной структуры организации и опыта внутри организации требования по независимости лиц и подразделений могут быть выполнены путем использования услуг сторонней организации. В свою очередь организации, которые имеют внутренние структуры с большим опытом в оценке рисков и применении Э/Э/ПЭ СБЗС систем и в которых эти структуры независимы и отделены (по управлению и используемым ресурсам) от тех структур, которые несут ответственность за основную разработку, могут использовать свои собственные ресурсы для удовлетворения требований к независимости организации.

2 Лицам, осуществляющим оценку функциональной безопасности, не рекомендуется предоставлять консультации по какому-либо вопросу, связанному с оценкой, поскольку это может поставить под угрозу их независимость.

8.2.17 Минимальные уровни независимости (см. таблицу 4) следует определять с учетом функции безопасности, выполняемой Э/Э/ПЭ СБЗС системой с наивысшим УПБ или подсистем (модулей) с наивысшей стойкостью к систематическим отказам, определенную в терминах УПБ.

Приложение А
(справочное)

Пример структуры документации

А.1 Общие положения

В настоящем приложении приведен пример структуры документации и метод формирования документов, необходимых для структурирования информации в соответствии с требованиями раздела 5. В документацию включают информацию, достаточную для эффективного выполнения:

- каждой стадии ЖЦ всей Э/Э/ПЭ СБЗС системы, АС и ПО (см. раздел 7);
- управления функциональной безопасностью (см. раздел 6);
- оценки функциональной безопасности (см. раздел 8).

Понятие достаточности информации зависит от ряда факторов, включая сложность и размер Э/Э/ПЭ СБЗС систем, а также требований, относящихся к конкретной области применения. Необходимая документация может быть определена в стандарте для соответствующей области применения.

Объем информации в каждом документе может изменяться от нескольких строк до многих страниц. Полный набор информации может быть разделен между несколькими физическими документами либо может быть представлен одним документом. Физическая структура документации зависит от размера и сложности Э/Э/ПЭ СБЗС систем, вида и уровня ответственности объекта и практики, сложившейся в организации и в конкретной области применения.

Пример структуры документации, приведенный в настоящем приложении, предназначен для иллюстрации возможного способа структурирования документации и возможного способа наименования документов. Документ представляет собой структурированный набор информации, предназначенной для восприятия человеком, пригодной для использования в качестве единицы обмена между пользователями и/или программируемыми системами. Данный термин применим не только к документам в традиционном смысле, но также и к таким понятиям, как файл данных или информация, хранящаяся в базе данных.

В настоящем стандарте термин «документ» в большей степени относится к информации, чем к физическим документам, если только иное не оговорено специально или не может быть понято в контексте раздела или подраздела, в котором используется этот термин. Документ может быть доступен для восприятия человеком в разных формах (например, на бумаге, пленке или ином носителе информации, допускающем ее представление на экране дисплея).

В примерах структуры документов, приводимых в настоящем приложении, документы определены в двух отношениях:

- тип документа;
- процесс или объект.

Тип документа характеризует содержание документа, например, описание функций или схема соединений. Процессы или объекты описывают собственно предметную область, например, схема управления турникетом.

Основными документами, определяемыми в настоящем приложении, являются:

- **акт** — содержит результаты выполненных работ;
- **диаграмма** — определяет функции с помощью диаграмм (символов и линий), представляющих сигналы, циркулирующие между символами;
- **журнал** — представляет информацию о событиях в хронологической форме;
- **запрос** — представляет описание запрашиваемых действий, которые должны быть подтверждены и затем специфицированы (например, запрос на техническое обслуживание);
- **инструкция** — содержит подробные указания о том, когда и как следует выполнять определенные действия (например, инструкция для оператора);
- **описание** — определяет планируемую или реальную функцию, устройство, характеристику или процесс (например, описание функции);
- **отчет** — описывает результаты процессов, таких как исследования, оценки, испытания и т. п. (например, отчет об испытаниях);
- **план** — содержит план того, когда, как и кем будут выполняться определенные действия (например, план технического обслуживания);
- **спецификация** — определяет необходимую функцию, характеристику или процесс (например, спецификация требований);
- **список** — представляет информацию в виде списка (например, список кодов, список сигналов).

Основной тип документа может иметь дополнение, уточняющее содержание, например, «спецификация требований» или «спецификация модулей АС».

А.2 Структура документов, относящихся к жизненному циклу системы

Таблицы А.1—А.3 содержат примеры структуры документации, предназначенной для структурирования информации в целях выполнения требований, установленных в разделе 5. Таблицы указывают стадии ЖЦ Э/Э/ПЭ СБЗС системы, которые преимущественно связаны с документами (обычно это стадии, в течение которых их разрабатывали). Названия документов в таблицах указаны в соответствии с А.1.

Таблица А.1 — Пример 1 структуры документации для информации, связанной с полным ЖЦ Э/Э/ПЭ СБЗС системы

Стадия полного ЖЦ Э/Э/ПЭ СБЗС системы	Информация
Разработка концепции	Описание (общая концепция)
Рассмотрение общей области определения СБЗС системы	Описание (область определения СБЗС системы)
Анализ опасностей и рисков	Описание (анализ опасностей и рисков)
Определение полных требований безопасности СБЗС системы	Спецификация (полные требования безопасности, включающие в себя: общие требования к функциям безопасности и общие требования к полноте безопасности)
Распределение общих требований безопасности	Описание (распределение полных требований безопасности по отдельным СБЗС и прочим средствам уменьшения риска)
Разработка требований к Э/Э/ПЭ СБЗС системам	Спецификация (требования к безопасности Э/Э/ПЭ СБЗС систем, содержащие требования к функциям безопасности и к полноте безопасности систем, их АС и ПО)
Общее планирование эксплуатации и технического обслуживания	План (эксплуатации и технического обслуживания)
Общее планирование подтверждения соответствия требованиям безопасности	План (подтверждения соответствия полным требованиям безопасности)
Планирование полной установки и ввода в эксплуатацию	План (полной установки и монтажа) План (ввода в действие)
Реализация (установка на объекте)	Акт (установки оборудования на объекте)
Полный монтаж и ввод в действие	Акт (полного монтажа). Отчет (ввод в действие)
Полное подтверждение соответствия требованиям функциональной безопасности	Отчет (подтверждение соответствия Э/Э/ПЭ СБЗС систем полным требованиям функциональной безопасности)
Эксплуатация и техническое обслуживание	Журнал (эксплуатации и технического обслуживания)
Видоизменения и модификация в целом	Запрос (на модификацию). Отчет (общая модификация и анализ влияния модифицированной системы). Журнал (видоизменений и модификаций)
Вывод из эксплуатации и утилизация	Отчет (анализ влияния вывода из эксплуатации и утилизации). План (вывода из эксплуатации и утилизации). Журнал (вывода из эксплуатации и утилизации)
Относится ко всем стадиям	План (обеспечения безопасности). План (проверок). Отчет (по проверкам). План (оценки функциональной безопасности). Отчет (оценка функциональной безопасности)

Таблица А.2 — Пример 2 структуры документации для информации, связанной с ЖЦ Э/Э/ПЭ СБЗС системы

Стадия ЖЦ Э/Э/ПЭ СБЗС системы	Информация
Планирование оценки соответствия Э/Э/ПЭ СБЗС системы	План (оценки соответствия Э/Э/ПЭ СБЗС системы)
Проектирование и создание Э/Э/ПЭ СБЗС системы	
Разработка ее структуры АС и архитектуры ПО	Описание (проект структуры Э/Э/ПЭ СБЗС системы, включая: структуру АС и архитектуру ПО). Программа [интегральных испытаний (тестирования) Э/Э/ПЭ модулей, подсистем СБЗС системы]. Программа [интегральных испытаний (тестирования) Э/Э/ПЭ СБЗС системы].
Структура АС	Описание (проект структуры АС). Программа (интегральных испытаний модулей, подсистем АС).
Структура модуля, подсистемы АС	Спецификация (проект модулей АС). Программа (испытаний модулей АС).
Создание и/или закупка составляющих (модулей) АС	Спецификация (модулей АС). Отчет [по испытаниям (тестированию) компонентов]
Интеграция подсистем в Э/Э/ПЭ СБЗС систему	Спецификация (интегрированной Э/Э/ПЭ СБЗС системы). Отчет (по испытаниям интегрированной СБЗС) (см. таблицу А.3)
Интеграция Э/Э/ПЭ СБЗС систем в КСБ	Спецификация (КСБ). Отчет [по испытаниям (тестированию) КСБ]
Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ СБЗС системы	Инструкция (по эксплуатации Э/Э/ПЭ СБЗС системы) Инструкция (по техническому обслуживанию Э/Э/ПЭ СБЗС системы)
Подтверждение соответствия Э/Э/ПЭ СБЗС системы	Отчет (подтверждение соответствия Э/Э/ПЭ СБЗС системы)
Подтверждение соответствия КСБ требованиям безопасности	Отчет (подтверждение соответствия КСБ требованиям безопасности)
Модификация (видоизменение) Э/Э/ПЭ СБЗС системы	Инструкция [по модификации (видоизменению) Э/Э/ПЭ СБЗС системы]. Запрос (на модификацию СБЗС системы). Отчет (анализ влияния модификации Э/Э/ПЭ СБЗС системы). Журнал (модификации Э/Э/ПЭ СБЗС системы)
Все стадии ЖЦ	План (обеспечения безопасности Э/Э/ПЭ СБЗС системы). План (верификации Э/Э/ПЭ СБЗС системы). Отчет (верификации Э/Э/ПЭ СБЗС системы). План (оценки функциональной безопасности Э/Э/ПЭ СБЗС системы). Отчет (по оценке функциональной безопасности Э/Э/ПЭ СБЗС системы)
Все стадии ЖЦ	Руководство по безопасности поставляемых составляющих

Таблица А.3 — Пример 3 структуры документации для информации, связанной с ЖЦ ПО Э/Э/ПЭ СБЗС системы

Стадия ЖЦ ПО	Информация
Требования к безопасности ПО Э/Э/ПЭ СБЗС системы	Требования (безопасности СБЗС ПО, включая: требования к функциям безопасности и требования к полноте безопасности)
Планирование оценки соответствия ПО. Разработка и создание ПО. Разработка архитектуры ПО. Разработка системы ПО. Разработка модулей ПО. Кодирование	План (оценки соответствия СБЗС ПО). Описание (разработанной архитектуры ПО) (см. описание разработки структуры АС). Программа (интегрального тестирования архитектуры ПО). Программа [интегральных испытаний (тестирования) АС и ПО]. Инструкция (руководство по средствам разработки и кодирования). Описание (разработка системы ПО). Программа (интегрального тестирования системы ПО). Спецификация (модулей ПО). Спецификация (тестов для модулей ПО). Список (исходные коды). Отчет (по проверке кодов)
Тестирование модулей ПО	Отчет (по тестированию модулей ПО)
Интеграция модулей ПО	Отчет (по тестированию интегрированных модулей ПО)
Интеграция ПО подсистемам Э/Э/ПЭ СБЗС системы	Отчет (по интегральному тестированию АС и ПО)
Процедуры эксплуатации и поддержки ПО	Инструкция (по установке ПО). Инструкция (по применению и поддержке ПО)
Подтверждение соответствия ПО	Отчет (по подтверждению соответствия ПО требованиям функциональной безопасности)
Модификация ПО	Инструкция (по процедурам модификации ПО). Запрос (на модификацию ПО). Отчет (анализ влияния модификации ПО) Журнал (модификации ПО)
Относится ко всем стадиям	План (обеспечения безопасности ПО). План (верификации ПО). Отчет (по верификации ПО). План (оценки функциональной безопасности ПО) Отчет (по оценке функциональной безопасности ПО)
Относится ко всем стадиям	Руководство по безопасности для поставляемых составляющих

В дополнение к документам, перечисленным в таблицах А.1, А.2 и А.3, могут быть разработаны дополнительные документы, дающие подробную дополнительную информацию или информацию, структурированную для конкретной цели, например, списки комплектующих изделий, списки сигналов, списки кабелей, таблицы кабельных соединений, диаграммы контуров управления, списки переменных.

Примечание — Примерами таких переменных служат уровни регулирования регуляторов, величины переменных для сигнализации, приоритеты в выполнении задач в компьютере. Некоторые из значений переменных могут быть предоставлены до поставки комплектующих изделий для систем, другие могут быть даны во время ввода в эксплуатацию или технического обслуживания систем.

А.3 Физическая структура документации

Физическая структура документации определяется способом, которым различные документы объединяют в документы, комплекты документов, книги и группы книг. Один и тот же документ может быть включен в разные комплекты.

Для больших и сложных систем многие физические документы объединяют в несколько книг. Для небольшой системы, имеющей невысокую сложность и ограниченное число физических документов, вся документация может быть объединена в одну книгу с закладками для различных комплектов документов. На рисунке А.1 показаны примеры таких групп книг, структурированных в соответствии с группами пользователей.

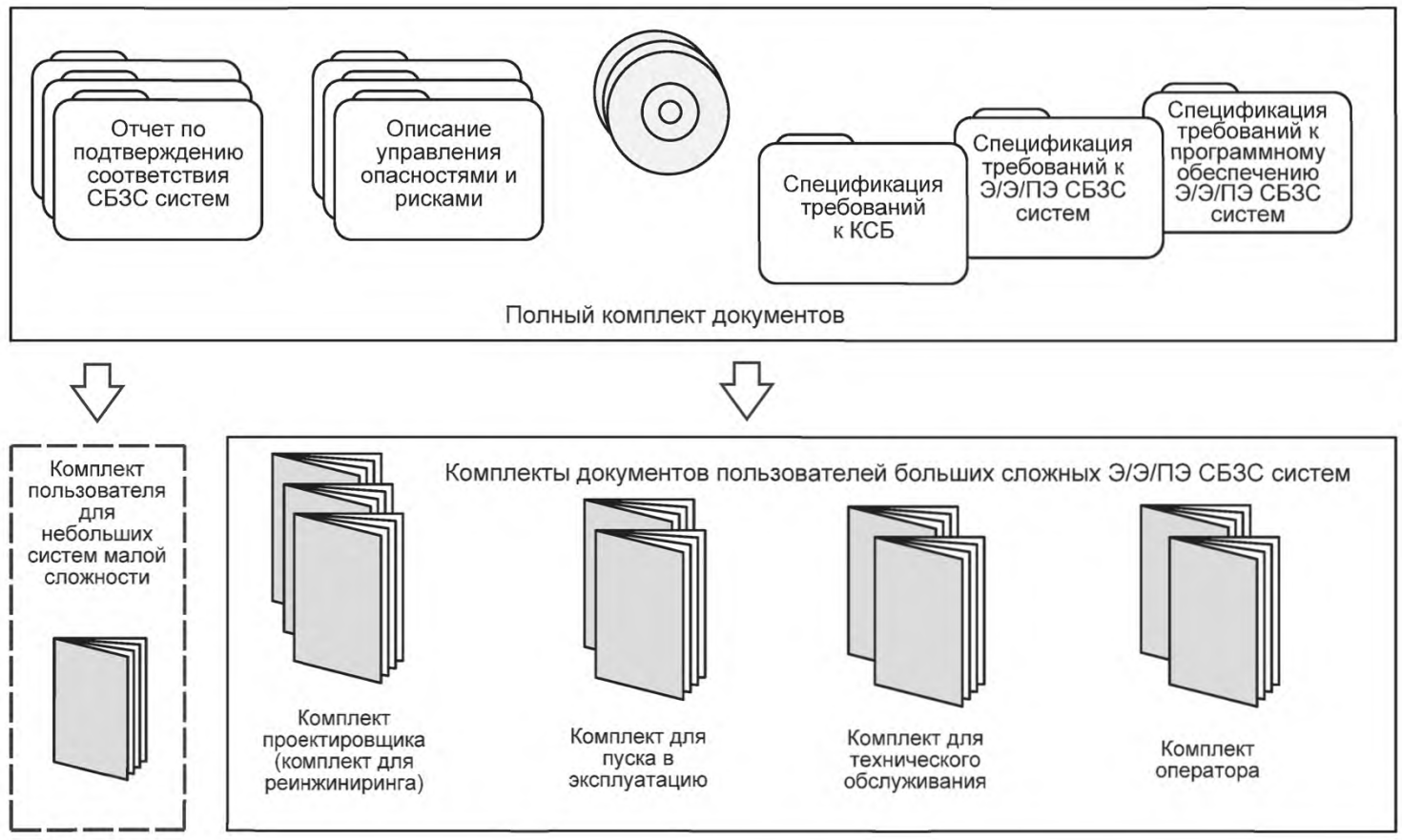


Рисунок А.1 — Примеры групп книг, структурированных в соответствии с группами пользователей

Библиография

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

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

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

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

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

http://www.iso.org/iso/ru/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53940 (доступ 24.09.2016).

УДК 621.5:814.8:006.354 МКС 13.100; 13.110; 13.200; 13.220; 13.310; 13.320; 91.120.99 NEQ

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

БЗ 8—2017/42

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 26.10.2018. Подписано в печать 13.11.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru