ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 22.1.14— 2013

Безопасность в чрезвычайных ситуациях

КОМПЛЕКСЫ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СТРУКТУРИРОВАННЫХ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ ИНЖЕНЕРНЫМИ СИСТЕМАМИ ЗДАНИЙ И СООРУЖЕНИЙ

Технические требования. Методы испытаний

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (Федеральный центр науки и высоких технологий) (ФГБУ ВНИИ ГОЧС (ФЦ)) совместно с Некоммерческим партнерством саморегулируемой организацией «Объединение организаций-разработчиков систем комплексной безопасности» (НП СРО «Объединение ОРСКБ»), Закрытым акционерным обществом «Инжиниринговый центр ГОЧС «БАЗИС» (ЗАО «ИЦ ГОЧС «БАЗИС»), Частным учреждением дополнительного профессионального образования «Учебно-консультационный центр гражданской обороны и чрезвычайных ситуаций «БАЗИС» (ЧУД ПО «УКЦ ГО и ЧС «БАЗИС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 71 «Гражданская оборона, предупреждение и ликвидация чрезвычайных ситуаций»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 октября 2013 г. № 1213-ст

4 В настоящем стандарте реализованы нормы Федеральных законов от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от ЧС природного и техногенного характера» [1], от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов» [2], от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений» [3], от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» [4], Постановлений Правительства Российской Федерации от 30 декабря 2003 г. № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» [5], от 24 марта 1997 г. № 334 «О порядке сбора и обмена в Российской Фе-дерации информацией в области защиты населения и территорий от ЧС природного и техногенного характера» [6], от 01 декабря 2009 г. № 982 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии» [7]

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0–2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) издаваемом информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru).

© Стандартинформ, 2014

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность в чрезвычайных ситуациях

КОМПЛЕКСЫ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СТРУКТУРИРОВАННЫХ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ ИНЖЕНЕРНЫМИ СИСТЕМАМИ ЗДАНИЙ И СООРУЖЕНИЙ

Технические требования. Методы испытаний

Safety in emergencies. Information-computational complexes of Structured system for monitoring and control of building / construction engineering equipment. Technical requirements. Test methods

Дата введения — 2014 — 07 — 01

1 Область применения

1.1 Настоящий стандарт распространяется на комплексы информационно-вычислительные структурированных систем мониторинга и управления инженерными системами зданий и сооружений (СМИС), предназначенные для применения в составе СМИС объектов для осуществления мониторинга и предупреждения чрезвычайных ситуаций природного и техногенного характера в соответствии с положениями ГОСТ Р 22.1.12–2005.

1.2 Настоящий стандарт устанавливает технические требования к комплексам информационно-вычислительным структурированных систем мониторинга и управления инженерными системами зданий и сооружений и методы их испытаний.

1.3 Положения настоящего стандарта предназначены для использования:

- федеральными органами исполнительной власти, входящими в единую государственную систему предупреждения и ликвидации чрезвычайных ситуаций (далее - РСЧС), и их территориальными органами;
- органами исполнительной власти субъектов Российской Федерации и местного самоуправления, в том числе органами, специально уполномоченными решать задачи по обеспечению мероприятий, направленных на решение задач гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, пожарной безопасности, осуществлению надзора и контроля в области защиты населения и территорий от чрезвычайных ситуаций (далее – органами ГОЧС);
- разработчиками комплексов информационно-вычислительных структурированных систем мониторинга и управления инженерными системами зданий и сооружений;
- застройщиками, техническими заказчиками, экспертными, надзорными, научно-исследовательскими, проектными, строительными, монтажными, эксплуатирующими организациями всех форм собственности, а также иными юридическими и физическими лицами – участниками инвестиционного процесса создания и эксплуатации СМИС.

1.4 Настоящий стандарт предназначен для оценки соответствия (сертификации) комплексов информационно-вычислительных структурированных систем мониторинга и управления инженерными системами зданий и сооружений требованиям, установленным настоящим стандартом.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.105–95 Единая система конструкторской документации. Общие требования к текстовым документам

ГОСТ 2.601–2006 Единая система конструкторской документации. Эксплуатационные документы

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

ГОСТ Р 8.568–97 Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения

ГОСТ 14254–96 Степени защиты, обеспечиваемые оболочками

ГОСТ 15150–69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

ГОСТ Р 15.201–2000 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения

ГОСТ 16962–71 Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний

ГОСТ 19091–2000 Замки и защелки для дверей. Методы испытаний

ГОСТ 19.105–78 Общие требования к программным документам

ГОСТ 19.301–79 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению

ГОСТ 19.401–78 Текст программы. Требования к содержанию и оформлению

ГОСТ 19.402–78 Описание программы

ГОСТ 19.501–78 Формуляр. Требования к содержанию и оформлению

ГОСТ 19.502–78 Описание применения. Требования к содержанию и оформлению

ГОСТ 19.503–79 Руководство системного программиста. Требования к содержанию и оформлению

ГОСТ 19.504–79 Руководство программиста. Требования к содержанию и оформлению

ГОСТ 19.505–79 Руководство оператора. Требования к содержанию и оформлению»

ГОСТ 19.507–79 «Ведомость эксплуатационных документов

ГОСТ 20.39.108–85 Стандартизация в Российской Федерации. Комплексная система общих технических требований. Требования по эргономике, обитаемости и технической эстетике. Номенклатура и порядок выбора

ГОСТ 21552–84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение

ГОСТ Р 22.1.02–95 Безопасность в чрезвычайных ситуациях. Мониторинг и прогнозирование. Термины и определения

ГОСТ Р 22.1.12–2005 Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования (с учетом Изменение №1)

ГОСТ Р 22.7.01–99 Безопасность в чрезвычайных ситуациях. Единая дежурно-диспетчерская служба. Основные положения

ГОСТ 24.701–86 Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения

ГОСТ 25861–83 Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний

ГОСТ 26828–86 Изделия машиностроения и приборостроения. Маркировка

ГОСТ 27.002–89 Надежность в технике. Основные понятия. Термины и определения

ГОСТ 27.003–90 Надежность в технике. Состав и общие правила задания требований по надежности

ГОСТ 27201–87 Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования

ГОСТ 28195–89 Оценка качества программных средств. Общие положения

ГОСТ 28806–90 Качество программных средств. Термины и определения

ГОСТ 34.201–89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.603–92 Информационная технология. Виды испытаний автоматизированных систем

ГОСТ Р 50739–95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50839–2000 Совместимость технических средств электромагнитная. Устойчивость средств вычислительной техники и информатики к электромагнитным помехам. Требования и методы испытаний

ГОСТ 5089–2003 Замки и защелки для дверей. Технические условия

ГОСТ Р 51072–2005 Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость

ГОСТ Р 51330.0–99 Электрооборудование взрывозащищенное. Часть 0. Общие требования

ГОСТ Р 52931–2008 Приборы контроля и регулирования технологических процессов. Общие технические условия

ГОСТ Р 52582–2006 Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому

Примечание:

1 При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя "Национальные стандарты" за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 22.0.02, ГОСТ Р 22.1.12, ГОСТ 28806, а также следующие термины с соответствующими определениями:

3.1 **внешние системы:** Автоматизированные системы органов повседневного управления РСЧС, в которые передаются сообщения СМИС.

3.2 **инцидент:** Критическое изменение контролируемых параметров систем инженерно-технического обеспечения и безопасности, технологических систем, инженерных (несущих) конструкций зданий и сооружений, природных процессов и явлений выше установленных допустимых уровней, которое может привести к аварии, чрезвычайной ситуации.

3.3 **работоспособное состояние оператора:** Состояние оператора, при котором он способен осуществлять определенную деятельность с требуемым качеством.

[ГОСТ 26387]

3.4 **режим реального времени:** Режим обработки информации, при котором обеспечивается взаимодействие системы обработки информации с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов.

[ГОСТ 15971]

4 Обозначения и сокращения

АИУС – автоматизированная информационно-управляющая система

АРМ – автоматизированное рабочее место

АСУ – автоматизированная система управления

ГОЧС – гражданская оборона и предупреждение чрезвычайных ситуаций

ДДС – дежурно-диспетчерская служба

ЕДДС – единая дежурно-диспетчерская служба

ЕСКД – единая система конструкторской документации

ПК – программный комплекс

ПМ ГОЧС – перечень мероприятий по гражданской обороне, мероприятий по предупреждению чрезвычайных ситуаций природного и техногенного характера

ПМИ – программа и методика испытаний

РСЧС – единая государственная система предупреждения и ликвидации чрезвычайных ситуаций

СМИК – система мониторинга инженерных (несущих) конструкций, опасных природных процессов и явлений

СМИС – структурированная система мониторинга и управления инженерными системами зданий и сооружений

ССП – подсистема сбора данных и передачи сообщений

СУБД – система управления базой данных

СУКС – подсистема связи и управления в кризисных ситуациях

ТЗ – техническое задание

ТУ – технические условия

ЦУКС – центр управления в кризисных ситуациях

ЧС – чрезвычайная ситуация

5 Технические требования

5.1 Требования к назначению, функциям и составу ИВК СМИС

5.1.1 Комплексы информационно-вычислительные структурированных систем мониторинга и управления инженерными системами зданий и сооружений (СМИС) предназначены для обеспечения мониторинга в составе СМИС объектов и информационной поддержки принятия решений органами повседневного управления РСЧС по предупреждению чрезвычайных ситуаций природного и техногенного характера, в т. ч. вызванных террористическими актами.

5.1.2 ИВК СМИС должны обеспечивать выполнение следующих функций:

- формирование и отображение сообщений СМИС, регламентов действий дежурного персонала объекта;
- непрерывный автоматический мониторинг в режиме реального времени изменения значений параметров, характеризующих состояния:

а) технологических систем, систем инженерно-технического обеспечения и безопасности (далее – контролируемых систем) объектов;

б) инженерных (несущих) конструкций зданий и сооружений объектов;

в) природных процессов и явлений;

- информирование в автоматическом режиме реального времени органов повседневного управления РСЧС о предаварийном, аварийном состоянии контролируемых систем, инженерных (несущих) конструкций зданий и сооружений, природных процессов и явлений;
- информационную поддержку принятия решений, позволяющих:

а) предупредить аварийную, чрезвычайную ситуацию, пожар;

б) не допустить развития аварийной, чрезвычайной ситуации, пожара;

в) не допустить / снизить потери, ущерб здоровью людей, материальные потери в случае развития аварийной, чрезвычайной ситуации, пожара;

г) обеспечить своевременное принятие мер по ликвидации последствий аварии, ЧС;

- автоматическое оповещение руководства объекта и служб эксплуатации объекта о предаварийном, аварийном состоянии контролируемых систем объекта, инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений;
- обеспечение связью экстренных оперативных, аварийных, аварийно-спасательных служб и формирований со штабом ликвидации последствий ЧС и пожара на объекте;
- проведение работ периодического и внеочередного мониторинга состояния инженерных (несущих) конструкций зданий и сооружений, природных процессов и явлений.

5.1.3 В состав ИВК СМИС входят:

- программно-технический комплекс сбора данных и передачи сообщений (ПТК ССП);
- программно-технический комплекс связи и управления в кризисных ситуациях (ПТК СУКС);
- программно-технический комплекс мониторинга инженерных (несущих) конструкций, опасных природных процессов и явлений (ПТК СМИК).

5.1.4 ПТК ССП должен обеспечивать выполнение следующих функций:

- непрерывный автоматический мониторинг в режиме реального времени изменения значений параметров состояния контролируемых систем;
- непрерывный прием от ПТК СМИК данных мониторинга инженерных (несущих) конструкций зданий и сооружений, природных процессов и явлений;
- контроль работоспособности оборудования ИВК СМИС и сопряжения с контролируемыми и внешними системами;
- контроль работоспособного состояния оператора СМИС;
- отображение данных мониторинга и контроля:

а) о параметрах состояния контролируемых систем объекта:

б) об инцидентах, авариях, ЧС, пожарах, террористических проявлениях;

в) об изменении состояния инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений;

г) о работоспособности и отказах оборудования ИВК СМИС и каналов сопряжения с контролируемыми и внешними системами;

д) от тревожных кнопок «Авария», «Тревога», «Пожар»;

- формирование и хранение базы данных мониторинга;
- поиск, редактирование и отображение архивных данных мониторинга;
- формирование и документирование отчетов о результатах мониторинга;
- создание и редактирование, импорт / экспорт классификаторов угроз аварий, ЧС;
- настройку и изменение режимов функционирования ИВК СМИС;
- формирование, хранение, отображение и передачу во внешние системы сообщений:

а) в автоматическом режиме о критическом изменении параметров контролируемых систем, инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений с характеристикой происшедшего события:

- инцидент;
- авария;
- пожар;
- тревога;
- о неработоспособности контролируемых систем;
- о нарушении топологии системы СМИС;
- о неработоспособном состоянии оператора СМИС;

а) в автоматизированном режиме:

- о чрезвычайной ситуации (по установленным формам);
- передачу в автоматическом режиме коротких сообщений (SMS) о критическом изменении контролируемых параметров по телефонным номерам.

5.1.5 ПТК ССП одновременно с формированием и отображением сообщений о критическом изменении контролируемых параметров должен обеспечивать отображение:

- регламента действий персонала ДДС объекта, соответствующего отображаемому сообщению;
- мест регистрации инцидентов, аварий, пожаров, террористических проявлений на 3D моделях объекта;
- мнемосхем СМИС объекта с отражением текущего состояния работоспособности основных компонентов ИВК СМИС;
- сведений, схем, планов, справочной информации (по запросу), включая:
- пути эвакуации;
- планы расположения основного оборудования и состояния систем инженерно-технического обеспечения на 3D модели объекта;
- схем путей подъезда к объекту;
- видеоинформации с места инцидента, аварии, пожара, тревоги.

5.1.6 ПТК СУКС должен обеспечивать:

- непрерывное устойчивое управление формированиями оперативных служб, аварийных, аварийно-спасательных служб (далее по тексту – аварийных служб) объекта в ходе ликвидации аварии, пожара, ЧС, в т.ч. вызванных террористическими актами (далее по тексту – в ходе ликвидации последствий);
- коммутацию оборудования СУКС, средств связи формирований аварийных служб объекта со средствами связи привлекаемых городских (муниципальных) аварийных служб, штабом ликвидации последствий и органами повседневного управления РСЧС;
- контроль состояния и передачу в ПТК ССП данных об изменении работоспособности и режимах работы оборудования ПТК СУКС и каналов связи, коммутируемых в ходе ликвидации последствий;
- дистанционное включение, управление режимами работы, коммутацию каналов связи и контроль работоспособности ПТК СУКС.

5.1.7 ПТК СМИК должен обеспечивать:

- непрерывный автоматический мониторинг в режиме реального времени изменения значений параметров состояния инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений;
- получение данных измерений, необходимых при обследовании зданий и сооружений при внеочередном или периодическом мониторинге;
- отображение данных мониторинга и результатов обработки;
- формирование и хранение базы данных мониторинга СМИК;
- поиск, редактирование и отображение архивных данных мониторинга СМИК;
- формирование и документирование отчетов о результатах мониторинга СМИК;
- настройку функционирования ПТК СМИК;
- контроль работоспособности оборудования ПТК СМИК;
- формирование, хранение, отображение, передачу в ПТК ССП и предоставление во внешние системы (при автономной работе) сообщений о состоянии и критическом изменении состояния инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений с характеристикой происшедшего события:
  - а) нарушение нормального состояния;
  - б) предаварийное состояние;
  - в) о неработоспособности оборудования СМИК;
  - г) о нарушении топологии СМИК объекта.

5.1.8 ПТК СМИК одновременно с формированием сообщений о критическом изменении состояния инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений должен обеспечивать отображение:

- регламента действий персонала ДДС объекта (при автономной работе);
- схемы инженерных (несущих) конструкций зданий и сооружений объекта;
- мест расстановки датчиков с отображением их состояния, номера и показаний на 3D моделях объекта;
- телеметрических данных параметров конструкций, процессов, явлений.

5.2 Требования к функциональным характеристикам ИВК СМИС

5.2.1 ИВК СМИС должен обеспечивать совместимость и информационно-техническое сопряжение с внешними системами в соответствии с техническими условиями (требованиями) на их подключение (сопряжение).

5.2.2 ИВК СМИС должен обеспечивать возможность передачи информации во внешние системы средствами различных сетей связи:

- проводной;
- радио;
- оптико-волоконной.

Допускается использовать каналы сети общего пользования, каналы в технологических сетях, выделенных сетях или сетях специального назначения.

5.2.3 В случае сбоя передачи информации во внешние системы (временного отсутствия соединения) ИВК СМИС должен обеспечивать:

- сохранность передаваемой информации в очереди (база данных);
- цикличный повтор попыток передачи информации из очереди вплоть до успешного завершения данной операции;
- очистку очереди при успешной передаче всей информации.

5.2.4 Средняя задержка в выдаче ИВК СМИС сообщений об инциденте, аварии, пожаре, изменении работоспособности СМИС с момента критического изменения параметров контролируемых систем объекта не должна превышать:

- на ДДС объекта – 15 с;
- во внешние системы – 30 с.

5.2.5 ИВК СМИС должен обеспечивать передачу во внешние системы не менее 1000 сообщений в час.

5.2.6 В ИВК СМИС должна быть предусмотрена возможность формирования и передачи в органы повседневного управления РСЧС сообщений о чрезвычайных ситуациях по установленным формам.

5.2.7 ИВК СМИС должен обеспечивать возможность оператору формировать сообщения о ЧС и отправлять их во внешние системы.

5.2.8 ИВК СМИС должен обеспечивать возможность наращивания (масштабирования) информационно-вычислительных ресурсов при изменении объёма мониторинга.

5.2.9 Системы управления базами данных, используемые в ИВК СМИС, должны соответствовать следующим требованиям:

- использование русского языка на уровнях пользовательского интерфейса;
- поддержка реляционной или объектно-реляционной модели базы данных;
- поддержка технологии клиент-сервер;
- поддержка многопроцессорной архитектуры;
- наличие средств создания индексов и кластеров данных;
- автоматическое восстановление базы данных;
- совместимость с операционными системами, используемыми для обеспечения функционирования СМИС объекта;
- поддержка сетевых протоколов TCP/IP;
- наличие графических средств администрирования;
- контроль доступа к данным;
- централизованное управление учетными записями пользователей.

5.2.10 Требования по диагностированию

5.2.10.1 В ИВК СМИС должно быть предусмотрено диагностирование:

- работоспособности ИВК СМИС;
- сопряжения ИВК СМИС с контролируемыми системами объекта;
- сопряжения ИВК СМИС с внешними системами;
- работоспособного состояния оператора СМИС путем получения автоматически отправляемых контрольных сообщений.

5.2.10.2 Средняя интенсивность отправки сообщений для контроля работоспособности должна быть не менее:

- 20 ч-1 – для контроля работоспособности оборудования ИВК СМИС объекта и его сопряжения с контролируемыми и внешними системами;
- 2 ч-1 – для контроля работоспособного состояния персонала ДДС СМИС.

5.2.10.3 Задержка времени формирования сообщений о нарушении работоспособности оборудования ИВК СМИС и его сопряжения с другими системами – не более 5 мин с момента получения последнего контрольного сообщения о работоспособности оборудования СМИС.

5.2.10.4 Задержка времени формирования сообщения о неработоспособном состоянии оператора СМИС (при отсутствии сигнала подтверждения) – не более 5 мин с момента получения последнего подтверждения о работоспособности.

5.2.10.5 Время ответа при контроле работоспособного состояния оператора СМИС объекта – не более 10 мин.

5.2.11 При превышении регламентированного времени на устранение инцидента в контролируемой системе объекта ИВК СМИС должен формировать, отображать и выдавать во внешние системы сообщение об аварии в данной системе.

5.2.12 ИВК СМИС должен обеспечивать функционирование СМИС объектов в следующих режимах:

- нормальный (автоматический режим работы, обеспечивающий непрерывное в режиме реального времени выполнение всех функций по предназначению);
- административный (сервисный режим для проведения обслуживания, реконфигурации и пополнения новыми компонентами);
- аварийный (восстановление функционирования в результате сбоя или отказа).

5.2.13 Получение данных измерений ПТК СМИК, необходимых при обследовании зданий и сооружений при внеочередном или периодическом мониторинге, не должно прерывать автоматический мониторинг в режиме реального времени изменения значений параметров состояния инженерных (несущих) конструкций зданий и сооружений объекта, природных процессов и явлений.

5.3 Требования к математическому, информационному, программному и лингвистическому обеспечению ИВК СМИС

5.3.1 Требования к математическому обеспечению ИВК СМИС

5.3.1.1 Математическое обеспечение ИВК СМИС должно обеспечивать выполнение требований 5.1 и 5.2 настоящего стандарта.

5.3.2 Требования к информационному обеспечению

5.3.2.1 Информационное обеспечение ИВК СМИС должно включать:

- описания экранных форм результатов выполнения функций (решения задач);
- классификатор угроз (инцидентов, аварий, пожаров и террористических проявлений) при формировании сообщений СМИС.

5.3.2.2 Кодировка, перечень и описания сообщений ИВК СМИС должны соответствовать «Классификатору угроз (инцидентов, аварий, пожаров, террористических проявлений) для формирования информационных сообщений СМИС», ведомственным словарям и классификаторам информации.

5.3.3 Требования к программному обеспечению ИВК СМИС

5.3.3.1 В состав программного обеспечения ИВК СМИС должны входить общее и специальное программные обеспечения функционирования ИВК СМИС в соответствии с требованиями 5.1 и 5.2 настоящего стандарта.

5.3.3.2 Программные средства ИВК СМИС должны соответствовать показателям качества, предусмотренным ГОСТ 28195: надежности, сопровождения, удобства применения, эффективности, универсальности, корректности.

5.3.4 Требования к лингвистическому обеспечению

5.3.4.1 ИВК СМИС должен иметь удобный, интуитивно понятный графический интерфейс.

5.3.4.2 Стиль оформления, качество графики диалоговых окон должны соответствовать стилю оформления используемой операционной системы.

5.3.4.3 Работа оператора с ИВК СМИС должно происходить в форме интерактивных манипуляций с экранными формами, встроенными меню.

5.4 Требования к электромагнитной совместимости

5.4.1 ИВК СМИС к воздействию электромагнитных помех должны иметь вторую степени жесткости по ГОСТ Р 50839-2000.

5.5 Требования к устойчивости ИВК СМИС

5.5.1 Устойчивость оборудования ИВК СМИС должна обеспечиваться механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

5.5.2 Оборудование ИВК СМИС должно размещаться в металлических или пластиковых шкафах (щитах, корпусах), обеспечивающих класс защиты не менее IP40 согласно ГОСТ 14254.

5.5.3 Замки, защелки, используемые в ИВК СМИС, по устойчивости к разрушающим воздействиям в зависимости от конструкции должны соответствовать требованиям ГОСТ Р 52582, ГОСТ 19091, ГОСТ 5089.

5.5.4 ИВК СМИС должен быть защищен от несанкционированного доступа в соответствии с требованиями не менее класса 3Б Руководящего документа Гостехкомиссии при Президенте РФ [9].

5.5.5 Требования по защите программного обеспечения ИВК СМИС должны обеспечиваться средствами ограничения, учета и администрирования доступа к операционным системам ИВК СМИС и разграничением доступа к ПО.

5.5.6 Доступ к ПО должен осуществляться с помощью паролей с разделением по типу пользователей:

- первый («администратор») – доступ ко всем функциям;
- второй («дежурный оператор») – доступ только к функциям текущего контроля;
- третий («системный оператор») – доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление ИВК СМИС.

5.5.7 Число буквенно-цифровых знаков в пароле должно быть не менее десяти.

5.5.8 При вводе пароля в систему вводимые знаки не должны отображаться на средствах отображения информации. После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем.

5.5.9 Для обеспечения информационной безопасности ИВК СМИС должны быть предусмотрено:

- установка межсетевого экрана (брандмауэра);
- установка антивирусного программного обеспечения;
- осуществление взаимодействия с внешними системами только по закрытой внешней сети (VPN);
- отсутствие незащищенных подключений к открытым сетям общего пользования (Интернет);
- защита программного обеспечения электронными ключами.

5.5.10 В ИВК СМИС должна быть обеспечена сохранность информации при следующих сбоях:

- сбой или выход из строя оборудования ИВК СМИС;
- сбои электропитания;
- сбой общесистемного программного обеспечения;
- сбой или отказ специального программного обеспечения;
- сбой из-за ошибок в работе оператора.

5.5.11 В ИВК СМИС должны быть предусмотрены средства автоматического резервного копирования информации, восстановления данных и программного обеспечения.

5.6 Требования к надежности

5.6.1 Значения показателей надежности ИВК СМИС должны быть не менее:

- коэффициент готовности – 99,8 %;
- средняя наработка на отказ ИВК СМИС объекта должна быть не менее 10000 ч.

5.6.2 Средний срок службы ИВК СМИС должен быть не менее 10 лет с учетом замены неисправных и выработавших свой ресурс компонент.

5.7 Требования устойчивости к внешним воздействующим факторам

5.7.1 Требования устойчивости ИВК СМИС в части воздействия климатических факторов устанавливаются в соответствии с климатическим исполнением по ГОСТ 15150.

5.7.2 Требования устойчивости ИВК СМИС к воздействию механических факторов устанавливаются в соответствии с условиями эксплуатации и группами исполнения изделий по ГОСТ 16962.

5.8 Требования к электропитанию

5.8.1 Электрооборудование ИВК СМИС по обеспечению надежности электроснабжения должно быть отнесено к особой группе первой категории в соответствии с классификацией «Правил устройств электроустановок» (ПУЭ) [10].

5.8.2 Основное электропитание средств ИВК СМИС должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В.

5.8.3 Средства ИВК СМИС должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15 % до плюс 10 %.

5.8.4 Силовые кабельные системы должны отвечать требованиям ПУЭ [10].

5.8.5 Средства ИВК СМИС должны быть снабжены резервным электропитанием при пропадании напряжения основного источника питания. Переход на резервное питание должен осуществляться автоматически без нарушения установленных режимов работы и функционального состояния средств ИВК СМИС.

5.8.6 Резервный источник питания должен обеспечивать выполнение основных функций системы при пропадании напряжений в сети на время не менее 2 ч.

5.8.7 При использовании в качестве источника резервного питания аккумуляторных батарей должна выполняться их автоматическая подзарядка.

5.8.8 При использовании в качестве источника резервного питания ИВК СМИС аккумуляторных или сухих батарей необходимо иметь индикацию разряда батареи ниже допустимого предела.

5.8.9 Эксплуатационная документация СМИС должна содержать раздел по обеспечению электробезопасности при монтаже, наладке и эксплуатации технических средств.

5.9 Требования безопасности

5.9.1 ИВК СМИС должен соответствовать общим требованиям безопасности по ГОСТ 12.2.007.0, ГОСТ Р МЭК 60065, ГОСТ 21552, ГОСТ 25861.

5.9.2 Оборудование ИВК СМИС должно иметь сертификаты по электробезопасности и электромагнитной безопасности по ГОСТ 12.1.019.

5.9.3 Материалы, комплектующие изделия, используемые в ИВК СМИС, должны быть экологически безопасны.

5.9.4 Оборудование ИВК СМИС должно соответствовать общим требованиям пожарной безопасности по ГОСТ 12.1.004.

5.9.5 Оборудование ИВК СМИС должно быть заземлено. Заземление должно быть выполнено в соответствии с ПУЭ [10].

5.9.6 Электрическое сопротивление изоляции средств ИВК СМИС между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными / выходными цепями должно быть не менее 1,0 МОм.

5.9.7 Уровни излучений ИВК СМИС должны соответствовать нормам и требованиям безопасности, установленным в ГОСТ 12.1.006.

5.9.8 Средства ИВК СМИС, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ГОСТ Р 51330.0 и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

5.10 Требования к конструкции

5.10.1 Габаритные размеры средств ИВК СМИС и их отдельных функционально и конструктивно законченных устройств и блоков должны обеспечивать транспортирование через типовые проемы зданий, сборку, установку и монтаж на месте эксплуатации.

5.10.2 Конструкции средств ИВК СМИС должны быть построены по модульному и блочно-агрегатному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных составных частей;
- удобство технического обслуживания, эксплуатации и ремонтопригодность;
- исключение возможности несанкционированного доступа к элементам управления параметрами;
- доступ ко всем элементам, узлам и блокам, требующим регулирования или замены в процессе эксплуатации.

5.10.3 Конструкционные, электроизоляционные материалы, покрытия и комплектующие изделия должны обеспечивать:

- механическую прочность;
- требуемую надежность;
- выполнение требований устойчивости к несанкционированным действиям по категориям и классам устойчивости;
- безопасную работу в заданных условиях эксплуатации.

5.11 Требования к маркировке

5.11.1 Маркировка ИВК СМИС должна быть выполнена в соответствии с ГОСТ 26828 и содержать:

- товарный знак и (или) другие реквизиты предприятия-изготовителя;
- условное обозначение средств ИВК СМИС;
- серийный номер;
- дату изготовления;
- знак сертификата соответствия (при наличии).

5.11.2 Маркировка средств ИВК СМИС при транспортировании в упаковке должна соответствовать ГОСТ 14192.

5.12 **Требования к документированию**

5.12.1 Конструкторская документация на ИВК СМИС должна соответствовать требованиям ЕСКД. Программная документация ИВК СМИС должна соответствовать требованиям ЕСКП. Эксплуатационные документы должны быть выполнены в соответствии с ГОСТ 2.601, ГОСТ 19.507 и ГОСТ 2.610.

6 Соответствие требованиям настоящего стандарта

6.1 Соответствие ИВК СМИС требованиям настоящего стандарта должно проводиться в сертифицированных лабораториях.

6.2 Соответствие ИВК СМИС требованиям настоящего стандарта не может декларироваться до тех пор, пока все испытания и проверки не будут выполнены.

6.3 Изготовитель должен представить достаточную информацию по всем разделам настоящего стандарта в случае, когда он декларирует, что параметры ИВК СМИС удовлетворяют установленным требованиям.

6.4 Изготовитель несет ответственность за то, что поставляемое оборудование ИВК СМИС и связанные с ним внешние устройства аналогичны образцу (ам), который (е) подвергался (ись) испытаниям согласно настоящему стандарту.

6.5 Существенные модификации оборудования ИВК СМИС должны обозначаться соответствующими индексами, маркировками, а также соответствовать требованиям настоящего стандарта.

7 Методы испытаний

7.1 **Общие положения**

7.1.1 Испытания ИВК СМИС проводят методами, приведенными в настоящем стандарте, а также по методам испытаний в соответствии с действующими нормативными документами на проведение сертификационных испытаний оборудования, входящего в состав ИВК СМИС.

7.1.2 Объем и последовательность испытаний устанавливают в программе и методике (ПМИ) сертификационных испытаний ИВК СМИС, утверждаемой органом по сертификации ИВК СМИС и согласованной с федеральным органом исполнительной власти, специально уполномоченным для решения задач в области защиты населения и территорий от чрезвычайных ситуаций.

7.1.3 Образцы средств ИВК СМИС, предназначенные для проведения испытаний, должны иметь техническую документацию в объеме, необходимом для проведения испытаний, и быть полностью укомплектованными.

7.1.4 При проведении испытаний ИВК СМИС должны быть обеспечены требования техники безопасности и другие условия в соответствии с требованиями нормативных документов.

7.1.5 Помещения для проведения испытаний должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование использоваться в соответствии с ПМИ сертификационных испытаний.

7.1.6 Приборы и оборудование, применяемые при проведении испытаний, должны быть аттестованы в соответствии с ГОСТ Р 8.568 и обеспечивать требуемую точность измерений.

7.1.7 Испытания ИВК СМИС должны проводиться в составе, указанном в 5.1.3.

7.1.8 Коэффициент охвата оборудования ИВК СМИС при испытаниях должен быть 100 %.

7.1.9 В ходе испытаний не должно быть:

- порчи аппаратуры;
- изменения операционных систем ИВК СМИС и программ тестирования и (или) порядка их выполнения;
- непреднамеренного изменения конфигурации ИВК СМИС и прикладных данных в памяти или данных обмена;
- ошибочного или непредсказуемого поведения базовой конфигурации ИВК СМИС.

7.1.10 Все испытания ИВК СМИС, кроме климатических, проводят в нормальных климатических условиях по ГОСТ 15150.

7.1.11 Соответствие конструктивным требованиям и информации, представленной изготовителем, должно быть оценено экспертизой, визуальным осмотром и (или) измерениями в соответствии с программой и методикой сертификационных испытаний ИВК СМИС.

7.2 **Испытания на соответствие ИВК СМИС требованиям к качеству программных средств**

7.2.1 Испытания ИВК СМИС на соответствие требованиям к качеству программных средств проводят в соответствии с ГОСТ 28195.

7.2.2 Качество программных средств определяется путем сравнения полученных расчетных значений показателей качества с соответствующими базовыми значениями в соответствии с методикой, представленной в ГОСТ 28195.

7.3 **Испытания ИВК СМИС на соответствие требованиям электромагнитной совместимости**

7.3.1 Испытания ИВК СМИС на соответствие требованиям электромагнитной совместимости проводят по ГОСТ Р 50839-2000.

7.4 **Испытания ИВК СМИС на устойчивость**

7.4.1 Испытания ИВК СМИС на устойчивость разрушающего воздействия проводят методами испытаний по ГОСТ Р 51072.

7.4.2 Испытания по защите программного обеспечения ИВК СМИС от несанкционированного доступа к информации и защите средств СВТ, входящих в состав ИВК СМИС, проводят проверкой на соответствие требованиям ГОСТ Р 50739.

7.4.3 Испытания ИВК СМИС на устойчивость к внешним воздействующим факторам проводят по ГОСТ Р 52931.

7.5 **Испытания ИВК СМИС на соответствие требованиям надежности**

7.5.1 Испытания ИВК СМИС на соответствие требованиям надежности проводят по методикам, разработанным с учетом положений и требований ГОСТ 27.003.

7.6 **Испытания ИВК СМИС на соответствие требованиям к электропитанию**

7.6.1 Испытания ИВК СМИС на соответствие требованиям к электропитанию проводят по методикам в соответствии с ТУ на электрооборудование ИВК СМИС.

7.7 **Испытания ИВК СМИС на соответствие требованиям безопасности**

7.7.1 Испытания ИВК СМИС на соответствие требованиям безопасности проводят по ГОСТ 21552-84.

7.8 **Испытания ИВК СМИС на соответствие требованиям к функциональным характеристикам**

7.8.1 Для каждого испытания в ПМИ должны быть:

- определены способы установки внешних соединений;
- разработаны тестовые программы испытаний;
- определены процедуры проверки правильности функционирования, включая методы оценки точности и временных отклонений параметров.

7.8.2 Все внутренние и внешние средства обмена данными, каналы ввода / вывода и коммуникаций ИВК СМИС должны быть задействованы.

7.8.3 Внешние устройства должны быть соединены через интерфейсы (контролеры) согласно техническим требованиям.

7.8.4 Датчики контроля изменения состояния инженерных (несущих) конструкций зданий и сооружений должны быть представлены по каждому типу в количестве, необходимом для функциональной проверки ИВК СМИС в полном объеме.

7.8.5 Характеристики различных режимов работы ИВК СМИС, такие как включение и останов, работа в нормальном и аварийном режимах, программирование / управление средствами наладки и тестирования и другие должны проверяться на качество исполнения и поведения.

7.8.6 Должны быть протестированы условия инициализации и перезагрузки всех компонентов ИВК СМИС в фазах запуска, нормальной работы и останова.

7.8.7 Проверка функциональных возможностей и показателей ИВК СМИС проводится методами формирования тестовых сигналов и сообщений от сопрягаемых средств и систем, контролеров, датчиков и устройств, проверки соответствия и качества результатов реакции и определением временных параметров реакции по методике, указанной в 7.8.8.

7.8.8 Методика проверки функциональных возможностей и показателей ИВК СМИС

7.8.8.1 Провести настройку и контроль работоспособности оборудования в соответствии с эксплуатационной документацией.

7.8.8.2 Сформировать тестовый сигнал (сообщение) о критическом изменении контролируемого параметра в зависимости от оконечного оборудования, системы, датчика, подключаемых к ИВК СМИС одним из следующих способов:

- изменением положения датчика (например, инклинометра);
- изменением контролируемого параметра (например, датчика температуры, подключенного к контролеру СМИС);
- имитацией сигнала, характеризующего критическое изменение контролируемого параметра с использованием устройства имитации, подключаемого к контролерам СМИС (например, имитацией изменения частоты собственных колебаний конструкции здания с использованием генератора частот, подключенного на вход канала акселерометра);
- формированием сообщений от контролируемых систем с использованием тестовых программ;
- другими способами, обеспечивающими проверку функциональных возможностей в полном объеме в соответствии с требованиями данного стандарта.
- одновременно с формированием тестового сигнала определить время реакции ИВК СМИС на критическое изменение контролируемых параметров.

7.8.8.3 Проверить реакцию на тестовый сигнал (сообщение) и оценить полноту отображаемой информации.

7.8.8.4 Повторить тестирование по каждому сигналу (показателю) не менее трех раз и результаты записать в протокол испытаний.

7.8.8.5 Параметры ИВК СМИС считаются соответствующими требованиям стандарта, если получены положительные результаты по всем тестовым испытаниям и время реакции на тестовые сигналы не превысило показателей, указанных в настоящем стандарте.

7.8.9 Проверка функциональных возможностей ИВК СМИС по обработке данных мониторинга по совокупности показателей контролируемых параметров осуществляется по методике, указанной в 7.8.10.

7.8.10 Методика проверки функциональных возможностей ИВК СМИС по обработке данных мониторинга по совокупности показателей.

7.8.10.1 Подключить к ИВК СМИС тестовое оборудование, обеспечивающее одновременное формирование сигналов (сообщений) о критическом изменении параметров нескольких контролируемых систем.

7.8.10.2 Одновременно инициировать сигналы (сообщения) от нескольких систем о превышении уровня контролируемых параметров «Инцидент».

7.8.10.3 Проверить реакцию на тестовые сигналы (сообщения) и оценить полноту отображаемой информации.

7.8.10.4 Повторить тестирование по различным комбинациям сигналов «Инцидент», «Авария» и результаты записать в протокол испытаний.

7.8.11 Параметры ИВК СМИС считаются соответствующими требованиям стандарта, если получены положительные результаты по всем тестовым испытаниям, информация отображается в полном объеме согласно эксплуатационной документации и время реакции на тестовые сигналы не превысило показателей, указанных в настоящем стандарте.

7.8.12 Проверка функциональных возможностей ПТК СУКС.

7.8.13 Проверка функциональных возможностей и показателей ПТК СУКС проводится методом контроля наличия и устойчивости связи, переключения и коммутации каналов связи, управления (переключения) режимов работы.

7.8.14 Проверка системы управления базами данных ИВК СМИС проводится методами анализа программной документации, определения наличия и полноты выполнения функций баз данных.

7.8.15 Проверка совместимости и информационно-технического сопряжения ИВК СМИС с внешними системами осуществляется в следующей последовательности.

7.8.15.1 ИВК СМИС подключается к тестовому оборудованию ПТК приема информации систем мониторинга и предупреждения чрезвычайных ситуаций природного и техногенного характера.

7.8.15.2 В соответствие с методикой, указанной в 7.8.8, на ИВК СМИС формируются сооб-

щения о критическом изменении параметров контролируемых систем.

7.8.15.3 На тестовом оборудовании ПТК приема информации систем мониторинга и предупреждения чрезвычайных ситуаций природного и техногенного характера определяется время реакция на переданное с ИВК СМИС сообщение, соответствие полученного сообщения переданному.

7.8.15.4 Проверка возможности автоматического и ручного формирования сообщений СМИС по запросу от ПТК приема информации осуществляется в соответствии с методикой, указанной в 7.8.8, посредством формирования, отправки тестовых запросов и контроля принятых сообщений от ИВК СМИС.

БИБЛИОГРАФИЯ

[1] Федеральный закон от 21 декабря 1994г. № 68-ФЗ — О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера

[2] Федеральный закон от 21 июля 1997 г. № 116-ФЗ — О промышленной безопасности опасных производственных объектов

[3] Федеральный закон от 30 декабря 2009 г. № 384-ФЗ — Технический регламент о безопасности зданий и сооружений

[4] Федеральный закон от 27 декабря 2002 г. № 184-ФЗ — О техническом регулировании

[5] Постановление Правительства Российской Федерации от 30 декабря 2003 г. № 794 — О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций

[6] Постановление Правительства Российской Федерации от 24 марта 1997 г. № 334 — О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера

[7] Постановление Правительства Российской Федерации от 01 декабря 2009 г. № 982 — Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии

[8] Постановление Правительства Российской Федерации от 21 мая 2007 г. № 304 — О классификации чрезвычайных ситуаций природного и техногенного характера

[9] Руководящий документ Гостехкомиссии при Президенте РФ от 30 марта 1992 г. — Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

[10] Приказ Минэнерго России от 08 июля 2002 г. № 204 — Правила устройства электроустановок (ПУЭ)

УДК 658.382.3:006.354 ОКС 13.110

Ключевые слова: информационно-вычислительный комплекс, структурированная система мониторинга и управления инженерными системами зданий и сооружений, дестабилизирующие факторы, угроза, авария, чрезвычайная ситуация, программно-технический комплекс, технические требования, методы испытания

Подписано в печать 01.04.2014. Формат 60x84 1/8.
Усл. печ. л. 2,33. Тираж 31 экз. Зак. 817.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»,

123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru