ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 22.1.03— 2019

Безопасность в чрезвычайных ситуациях

СИСТЕМА МОНИТОРИНГА ИНЖЕНЕРНЫХ СИСТЕМ ЗДАНИЙ И СООРУЖЕНИЙ

Технические требования. Протоколы информационного обмена

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций» (Федеральный центр науки и высоких технологий) (ФГБУ ВНИИ ГОЧС (ФЦ)), Обществом с ограниченной ответственностью Научно-производственное объединение «Диагностика и анализ риска» (ООО НПО «ДИАР») и Обществом с ограниченной ответственностью «Научно-технический центр «Технологии и безопасности» (ООО «НТЦ «ТБ»)

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 14 ноября 2019 г. № 1158-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) 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 (www.gost.ru)

© Стандартинформ, оформление, 2019

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 2
3 Термины и определения . . . 2
4 Сокращения и обозначения . . . 3
5 Общие положения . . . 3
6 Идентификационный ключ объекта . . . 5
7 Аутентификация программного комплекса системы мониторинга инженерных систем зданий и сооружений . . . 5
8 Защита передаваемых сообщений . . . 6
9 Классы сообщений . . . 6
9.1 События (происшествия) . . . 6
9.2 Сообщения о событиях (происшествиях), формируемые оперативным персоналом системы мониторинга инженерных систем задний и сооружений . . . 7
9.3 Контрольные сообщения программного комплекса системы мониторинга инженерных систем зданий и сооружений . . . 8
9.4 Сообщения о регламентных работах . . . 9
9.5 Проверка подключения . . . 10
10 Классификатор событий (происшествий) . . . 10
Приложение А (обязательное) Унифицированная WSDL-схема веб-сервиса программного комплекса систем мониторинга инженерных систем зданий и сооружений и программного комплекса приема информации от систем мониторинга инженерных систем зданий и сооружений объектов органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций . . . 12
Приложение Б (справочное) Примеры сообщений о событиях (происшествиях), происходящих на объекте мониторинга . . . 17
Приложение В (справочное) Примеры сообщений о проведении проверки готовности оперативного персонала и программного комплекса системы мониторинга инженерных систем зданий и сооружений . . . 20
Приложение Г (справочное) Примеры сообщений о проведении регламентных работ на объекте мониторинга . . . 21
Приложение Д (справочное) Примеры сообщений о проверке соединения между программным комплексом системы мониторинга инженерных систем зданий и сооружений и программным комплексом приема информации от систем мониторинга инженерных систем зданий и сооружений объектов органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций . . . 23
Приложение Е (справочное) XSD-схема списка событий (происшествий) . . . 24
Приложение Ж (справочное) Пример списка событий (происшествий) . . . 26
Приложение И (обязательное) Классификатор угроз системы мониторинга инженерных систем зданий и сооружений объектов . . . 29
Приложение К (рекомендуемое) Рекомендуемые перечень, кодировка событий (инцидентов, аварий, пожаров, террористических проявлений, чрезвычайных ситуаций) и состав контролируемых параметров для формирования информационных сообщений в рамках взаимодействия систем мониторинга инженерных систем зданий и сооружений объектов различного типа и органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций . . . 32
Библиография . . . 43

Введение

Настоящий стандарт разработан для организации информационного взаимодействия систем мониторинга инженерных систем зданий и сооружений (СМИС), функционирующих в составе автоматизированных систем органов повседневного управления (ОПУ) Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность в чрезвычайных ситуациях

СИСТЕМА МОНИТОРИНГА ИНЖЕНЕРНЫХ СИСТЕМ ЗДАНИЙ И СООРУЖЕНИЙ

Технические требования. Протоколы информационного обмена

Safety in emergencies. System for monitoring of buildings/constructions engineering equipment. Technical requirements. Communication protocols

Дата введения — 2020—04—01

1 Область применения

1.1 Настоящий стандарт распространяется на программные комплексы систем мониторинга инженерных систем зданий и сооружений (ПК СМИС), предназначенные для применения в составе органов повседневного управления (ОПУ) различных уровней (объектового, муниципального, регионального, федерального) территориальной подсистемы, а также функциональных подсистем Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) для осуществления мониторинга и предупреждения чрезвычайных ситуаций природного и техногенного характера в случаях, предусмотренных федеральными законами, нормативными правовыми актами Правительства Российской Федерации и соответствующего субъекта Российской Федерации.

1.2 Настоящий стандарт устанавливает общие технические требования к протоколам межуровневого информационного обмена ПК СМИС. Положения настоящего стандарта могут применяться для оценки соответствия ПК СМИС требованиям, предъявляемым к информационной совместимости и организации информационного обмена.

1.3 Положения настоящего стандарта предназначены для использования:

- органами, уполномоченными на решение задач в области защиты населения и территорий от чрезвычайных ситуаций;
- органами исполнительной власти субъектов Российской Федерации и местного самоуправления;
- органами повседневного управления РСЧС всех уровней: объектовыми, муниципальными, региональными, межрегиональными, федеральными;
- 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;
- разработчиками ПК СМИС;
- контрольно-надзорными органами Ростехнадзора (в областях промышленной безопасности, строительного надзора, использования атомной энергии) и МЧС России (в области пожарной безопасности, гражданской обороны и защиты населения и территорий от чрезвычайных ситуаций).

1.4 Все ПК СМИС, применяемые в ОПУ РСЧС различного уровня, должны иметь подтверждение соответствия требованиям настоящего стандарта. Подтверждение соответствия выполняется в соответствии с требованиями законодательства о техническом регулировании.

1.5 Требования к ПК СМИС, включая технические требования, требования к основным компонентам (видам обеспечения) СМИС по ГОСТ 34.003, требования к каналам информационного обмена ОПУ РСЧС различного уровня не являются предметом настоящего стандарта и регламентируются другими нормативными документами.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ Р 22.0.02 Безопасность в чрезвычайных ситуациях. Термины и определения

ГОСТ Р 55201 Безопасность в чрезвычайных ситуациях. Порядок разработки перечня мероприятий по гражданской обороне, мероприятий по предупреждению чрезвычайных ситуаций природного и техногенного характера при проектировании объектов капитального строительства

ГОСТ Р ИСО/МЭК 7498-1 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт 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 55201, ГОСТ Р ИСО/МЭК 7498-1, а также следующие термины с соответствующими определениями:

3.1

орган повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций; ОПУ РСЧС: Организация (подразделение), создаваемое федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями для обеспечения их деятельности в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и выделяемыми (привлекаемыми) для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях.

[ГОСТ Р 22.0.02—2016 статья 2.2.4]

3.2 **программные комплексы систем мониторинга инженерных систем зданий и сооружений;** ПК СМИС: Программные комплексы специализированных автоматизированных систем объекта, предназначенные для осуществления мониторинга состояния инженерных систем объекта и предупреждения чрезвычайных ситуаций природного и техногенного характера, информационно сопряженные с автоматизированными системами органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций.

3.3 **программный комплекс приема информации от систем мониторинга инженерных систем зданий и сооружений объектов;** ПК РСЧС: Программный комплекс приема информации от систем мониторинга инженерных систем зданий и сооружений объектов, функционирующий в составе автоматизированных систем органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций уровней выше объектового (муниципального, регионального, федерального уровней территориальной подсистемы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, а также функциональных подсистем единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций).

4 Сокращения и обозначения

В настоящем стандарте применены следующие сокращения:

АСУ ТП — автоматизированная система управления технологическими процессами;

АХОВ — аварийно химически опасные вещества;

ГТС — гидротехническое сооружение;

ОБВ — опасные биологические вещества;

ОИАЭ — объекты использования атомной энергии;

ОПО — опасный производственный объект;

ОПУ РСЧС — органы повседневного управления РСЧС;

ПК — программный комплекс;

РВ — радиоактивные вещества;

РСЧС — Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций;

СМИС — система мониторинга инженерных систем зданий и сооружений;

ЧС — чрезвычайная ситуация;

ЭЦП — электронно-цифровая подпись.

5 Общие положения

5.1 В настоящем стандарте излагаются требования к информационному обмену (взаимодействию) ПК СМИС, функционирующих в составе автоматизированных систем ОПУ РСЧС различного уровня.

По функциональному назначению и решаемым задачам различаются ПК СМИС, обеспечивающие непосредственный мониторинг состояния объектов мониторинга, и ПК приема информации от СМИС объектов, функционирующие в составе ОПУ РСЧС различных уровней (ПК РСЧС).

5.2 Обмен данными между ПК СМИС и ПК РСЧС осуществляется средствами различных транспортных сетей по протоколу Ethernet стандарта IEEE 802. На транспортном и сетевом уровнях взаимодействия (по семиуровневой модели OSI по ГОСТ Р ИСО/МЭК 7498-1) используется стандартизованный стек протоколов TCP/IP.

На прикладном уровне информационный обмен осуществляется по протоколу HTTP в формате SOAP [1], [2] формализованными сообщениями установленного формата, представленными в виде электронного документа, сформированного посредством расширяемого языка разметки Extensible Markup Language (XML). При декларации кодировки, являющейся частью декларации XML, используются названия и псевдонимы русскоязычных наборов символов, зарегистрированных в Internet Assigned Numbers Authority (IANA).

Информационный обмен ведется с использованием средств криптозащиты, обеспечивающей подтверждение подлинности информации, и сторон, участвующих в обмене.

5.3 Взаимодействие ПК СМИС с ПК РСЧС осуществляется посредством веб-сервиса, который предоставляется программным веб-сервером, действующим в составе ПК РСЧС. Для доступа к веб-сервису используется URL-адрес gost.e-ecolog.ru , где host — IP-адрес сервера, к которому ПК СМИС осуществляет подключение, port — адрес порта для доступа к веб-серверу ПК РСЧС.

Для описания информационного взаимодействия ПК СМИС с ПК РСЧС используется унифицированная схема WSDL [3], описывающая контракт веб-сервиса и доступная по адресу gost.e-ecolog.ru monitoring/node/dispatch.wsdl.

5.4 На прикладном уровне (по семиуровневой модели OSI по ГОСТ Р ИСО/МЭК 7498-1) используется протокол HTTP, который выполняет роль транспорта для протокола SOAP.

5.5 Веб-сервис поддерживает передачу следующих видов сообщений, обеспечивающих передачу информации:

- DispatchMessage — о событиях (происшествиях), происходящих на объекте мониторинга;
- DispatchMaintenance — о проведении регламентных работ на объекте мониторинга;
- DispatchControlPoint — о проведении проверки готовности оперативного персонала и ПК СМИС;
- Test — о проведении проверки соединения между ПК СМИС и ПК РСЧС.

Адреса веб-сервиса приведены в таблице 1.

Таблица 1 — Сообщения веб-сервиса

Виды сообщений	Адрес веб-сервиса
DispatchMessage	gost.e-ecolog.ru
DispatchMaintenance	gost.e-ecolog.ru g/schemas/node/DispatchMaintenanceRequest
DispatchControlPoint	gost.e-ecolog.ru
Test	gost.e-ecolog.ru

5.6 Предусмотрен следующий порядок информационного обмена:

- ПК СМИС формирует сообщение и передает его в ПК РСЧС;
- ПК РСЧС обрабатывает полученное сообщение и формирует сообщение для ПК СМИС, свидетельствующее об успешности обработки полученного сообщения.

В случае ошибки при обработке ПК СМИС может повторить передачу сообщения или отобразить на автоматизированном рабочем месте СМИС объекта сообщение о невозможности передачи сообщения (см. рисунок 1).

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<SOAP-ENV:Fault xmlns:SOAP-ENV="gost.e-ecolog.ru >
<faultcode>SOAP-ENV:Client</faultcode>
<faultstring xml:lang="en">Validation error</faultstring>
<detail></detail>
</SOAP-ENV:Fault>
```

Рисунок 1 — Структура xml-сообщения, содержащего сведения об ошибке

5.7 Подключение ПК СМИС к ПК РСЧС выполняется в следующей последовательности:

- в ПК РСЧС регистрируется подключаемый ПК СМИС, для которого автоматически формируется идентификационный номер;
- идентификационные данные объекта сохраняются в файл (далее — идентификационный ключ) и передаются в ПК СМИС. Формат идентификационного ключа описан в разделе 6;
- ПК РСЧС предоставляет ПК СМИС сертификат безопасности X.509 [4], [5], содержащий открытый ключ;
- ПК СМИС предоставляет ПК РСЧС собственный сертификат безопасности X.509, содержащий открытый ключ ПК СМИС;
- ПК СМИС предоставляет ПК РСЧС классификатор событий (происшествий), содержащий список угроз, возможных на объекте мониторинга, а также регламент действий оператора, при возникновении каждой из них. Формат классификатора событий (происшествий) детально описан в разделе 10;
- WSDL — схема веб-сервиса ПК РСЧС приведена в приложении А.

5.8 В процессе информационного взаимодействия между ПК СМИС и ПК РСЧС возможно возникновение ошибок, приведенных в таблице 2.

Таблица 2 — Текст (шаблон) сообщений об ошибках с описаниями

Текст (шаблон) сообщения об ошибках	Описание
No WS-Security header found	ПК СМИС передает сообщение в открытом виде, без использования шифрования и цифровой подписи
cvc-complex-type.2.4.a: Invalid content was found starting with element ''. One of '{"http:// host:port /monitoring/ schemas/node":}' is expected.	Сообщение, передаваемое ПК СМИС в ПК РСЧС, сформировано некорректно
The certificate used for the signature is not trusted	X.509 сертификат ПК СМИС не зарегистрирован в ПК РСЧС
No certificates were found for encryption	В ПК СМИС не установлен X.509 сертификат ПК РСЧС

6 Идентификационный ключ объекта

6.1 Идентификационный ключ включает в себя идентификационный номер (Identifier) и идентификационное имя (Name) объекта.

Идентификационный номер формируется автоматически при регистрации объекта в ПК РСЧС и используется для идентификации сообщений, поступающих в ПК РСЧС от ПК СМИС.

6.2 Идентификационный ключ выгружается в файл установленного формата и передается на объект мониторинга с целью использования при формировании сообщений, передаваемых в ПК РСЧС.

Описание элементов идентификационного ключа приведено в таблице 3.

Таблица 3 — Состав идентификационного ключа (расшифровка полей xml-файла)

Элемент	Тип данных	Обязательное	Описание
Name	Строка	Да	Наименование объекта в ПК РСЧС
Identifier	Строка	Да	Идентификационный номер объекта мониторинга в ПК РСЧС

На рисунке 2 представлен пример файла, содержащего идентификационный ключ.

```
<?xml version="1.0" encoding="UTF-8" ?>
<MonitoringObject>
<Name> Объект мониторинга </Name>
<Identifier>1c04fd70-5359-40de-a1cb-cf86616a333b </Identifier>
</MonitoringObject>
```

Рисунок 2 — Пример файла, содержащего идентификационный ключ

7 Аутентификация программного комплекса системы мониторинга инженерных систем зданий и сооружений

7.1 Перед началом взаимодействия ПК СМИС и ПК РСЧС должны обменяться открытыми ключами (сертификат X.509), которые в процессе обмена сообщениями будут использованы для шифрования и цифровой подписи передаваемых сообщений.

Обе схемы (ЭЦП и шифрование) применяют для передачи всех типов сообщений.

7.2 Для сертификата X.509 ПК СМИС должны быть заданы ключи со следующими областями применения (поле Key Usage):

- dataEncipherment ключ может быть использован для целей обеспечения конфиденциальности и целостности информации;
- keyEncipherment ключ может быть использован для шифрования других ключей;
- digitalSignature ключ может быть использован для целей обеспечения целостности и авторства информации, формирования и проверки ЭЦП электронных документов и информации, установления идентичности в процессе аутентификации.

7.3 При формировании и отправке сообщения от ПК СМИС в ПК РСЧС:

- формируется сообщение;
- шифруется сообщение с использованием открытого ключа ПК РСЧС;
- подписывается сообщение с использованием закрытого ключа ПК СМИС;
- отправляется сообщение в ПК РСЧС.

7.4 При приеме и обработке сообщения, полученного ПК РСЧС от ПК СМИС выполняется:

- проверка сертификата ПК СМИС;
- проверка цепочки доверенных сертификатов;
- проверка списка отозванных сертификатов;
- расшифровка сообщения закрытым ключом ПК РСЧС;
- проверка цифровой подписи сообщения с использованием открытого ключа ПК СМИС;
- обработка сообщения;

- формирование ответа;
- шифрование ответа с использованием открытого ключа ПК СМИС;
- подписка ответа закрытым ключом ПК РСЧС;
- отправка ответа в ПК СМИС.

8 Защита передаваемых сообщений

8.1 ПК РСЧС использует спецификацию WS-Security, описывающую дополнения к обмену сообщениями по протоколу SOAP, для защиты передаваемых сообщений. Данный подход позволяет обеспечить целостность и конфиденциальность передаваемых данных.

8.2 Для обмена применяется схема с обеспечением безопасности на уровне сообщения, когда вся информация, относящаяся к системе защиты, скрывается (инкапсулируется) в SOAP — сообщении. Пример SOAP-сообщения приведен в приложении Б.

8.3 Схема обмена сообщениями с использованием шифрования реализована следующим образом:

- ПК СМИС, используя открытый ключ ПК РСЧС, шифрует передаваемое сообщение;
- ПК РСЧС, используя свой закрытый ключ, расшифровывает полученное сообщение;
- ПК РСЧС, используя открытый ключ ПК СМИС, шифрует ответное сообщение;
- ПК СМИС, получив от ПК РСЧС ответное сообщение, расшифровывает его, используя свой закрытый ключ.

8.4 Обмен сообщениями с использованием ЭЦП выполняется в следующей последовательности:

- ПК СМИС подписывает передаваемое сообщение с использованием своего закрытого ключа;
- ПК РСЧС, используя открытый ключ ПК СМИС, проверяет целостность полученного сообщения;
- ПК РСЧС, используя собственный закрытый ключ, подписывает ответное сообщение, передаваемое ПК СМИС;
- ПК СМИС, используя открытый ключ ПК РСЧС, проверяет целостность полученного сообщения.

9 Классы сообщений

9.1 События (происшествия)

9.1.1 События (происшествия) — класс сообщений, генерируемый ПК СМИС, предназначенный для уведомления ПК РСЧС о событиях (происшествиях), происходящих на объекте мониторинга. Структура сообщения описана в таблице 4.

Таблица 4 — Расшифровка полей сообщения класса «Событие (происшествие)»

Элемент	Тип данных	Обязательное поле	Описание
Number	GUID	Да	Идентификатор сообщения
Source	GUID	Нет	Идентификатор исходного сообщения. Используется для построения цепочки сообщений, привязанных к одному событию
ObjectIdentifier	Строка	Да	Регистрационный номер объекта в ПК РСЧС, содержащийся в идентификационном ключе объекта
ObjectName	Строка	Да/нет	Наименование объекта в ПК РСЧС, содержащееся в идентификационном ключе объекта
IncidentType	Строка	Да	Код события согласно классификатору угроз (см. п.10.4)
IncidentTypeName	Строка	Да/нет	Наименование события
IncidentStatus	Строка	Да	Код текущего состояния события. Список возможных значений приведен в таблице 5
IncidentStatusName	Строка	Да/нет	Текстовое значение, описывающее текущее состояние события

Окончание таблицы 4

Элемент	Тип данных	Обязательное поле	Описание
Text	Строка	Нет	Дополнительная информация, касающаяся текущего состояния события
Time	Дата/время	Да	Время изменения состояния события
Path	Строка	Нет	Место регистрации события

9.1.2 В случае возникновения на объекте события (происшествия) ПК СМИС формирует для ПК РСЧС сообщение с кодами «Инцидент», или «Авария», или «Тревога», или «Пожар» (см. таблицу 5).

Таблица 5 — Коды состояний элементов IncidentStatus и IncidentStatusName

IncidentStatus	IncidentStatusName	Текстовое описание
100	INCIDENT	Инцидент
110	DAMAGE	Авария
120	ALERT	Тревога
130	FIRE	Пожар
200	SAFETY	Снятие с регистрации

9.1.3 Если событие (происшествие) не подтвердилось или устранено, ПК СМИС формирует сообщение с кодом 200 «Снятие с регистрации» (см. таблицу 5).

9.1.4 Примеры сообщений о событиях (происшествиях) приведены в приложении Б.

9.1.5 Код события присваивается согласно классификатору угроз (см. пункт 10.4).

9.1.6 После возникновения события с кодом «Инцидент» ПК СМИС включает отслеживание последовательности дальнейшего изменения состояния соответствующего(их) параметра(ов), связанного(ых) с событием (происшествием), и должен следить за построением цепочки сообщений, привязанных к событию (происшествию), и за трансформацией состояния события (происшествия) (например, инцидент ⇢ авария ⇢ инцидент ⇢ снятие с регистрации).

9.2 Сообщения о событиях (происшествиях), формируемые оперативным персоналом системы мониторинга инженерных систем задний и сооружений

9.2.1 События (происшествия), сообщения о которых формируются оперативным персоналом, — класс сообщений, генерируемый ПК СМИС на основе решения оперативного персонала и формируемый в автоматизированном режиме, для уведомления ПК РСЧС о событиях, происходящих на объекте мониторинга. Структура сообщения приведена в таблице 4.

9.2.2 Для кодировки сообщений, формируемых оперативным персоналом по факту события (происшествия), ПК СМИС формирует сообщения с элементом IncidentType с кодами, перечисленными в таблице 6.

Таблица 6 — Кодировка элемента IncidentStatus для сообщений, формируемых оперативным персоналом по факту события (происшествия)

IncidentStatus	Текстовое описание
111	Авария — сообщение, формируемое оперативным персоналом
121	Тревога — сообщение, формируемое оперативным персоналом
131	Пожар — сообщение, формируемое оперативным персоналом

9.2.3 Примеры сообщений, формируемых оперативным персоналом по факту события (происшествие), приведены в приложении Б.

9.3 Контрольные сообщения программного комплекса системы мониторинга инженерных систем зданий и сооружений

9.3.1 Контрольные сообщения — класс сообщений, генерируемый ПК СМИС, предназначенный для уведомления ПК РСЧС о проверках готовности оперативного персонала и ПК СМИС, проводимых на объекте мониторинга. Структура сообщения представлена в таблице 7.

Таблица 7 — Структура (расшифровка полей) контрольных сообщений

Поле	Тип данных	Обязательное	Описание
Number	GUID	Да	Идентификатор сообщения
MonitoringObject	Строка	Да/нет	Наименование объекта в ПК РСЧС, содержащееся в идентификационном ключе объекта
MonitoringObjectIdentifier	Строка	Да	Регистрационный номер объекта в ПК РСЧС, содержащийся в идентификационном ключе объекта
ControlType	Строка	Да	Вид контрольной проверки: - ПК СМИС; - оперативный персонал СМИС
ControlStatus	Строка	Да	Текущий статус контрольной проверки: - запрос готовности; - подтверждение готовности
RequestTime	Дата/время	Да	Время выполнения контрольной проверки
AcknowledgementTime	Дата/время	Нет	Время получения готовности оперативного персонала СМИС
ValidityTime	Дата/время	Нет	Время действия проверки (ПК СМИС определяет, в течение какого времени данная проверка считается пройденной)

9.3.2 В момент начала проведения контрольной проверки ПК СМИС отправляет сообщение с кодом «Запрос готовности» в поле ControlStatus с указанием времени начала проверки. В случае подтверждения готовности в адрес ПК РСЧС отправляется сообщение с кодом «Подтверждение готовности», в котором содержится время подтверждения готовности и время, в течение которого данная проверка считается действительной.

9.3.3 Время проведения контрольных проверок (периодичность проверки) определяется ПК СМИС при проектировании (вводе в действие) ПК СМИС в зависимости от особенности объектов мониторинга и специфики объекта, на котором установлена СМИС. Рекомендуемое время проведения контрольной проверки (не реже): готовности оператора — 30 мин, готовности ПК СМИС — 20 мин.

9.3.4 Коды видов и статусов контрольной проверки представлены в таблицах 8 и 9 соответственно.

Таблица 8 — Коды видов контрольной проверки

Код	Значение
OFFICER	Контрольная проверка готовности оперативного персонала СМИС
SERVICE	Контрольная проверка работоспособности систем ПК СМИС

Таблица 9 — Коды статуса контрольной проверки

Код	Значение
REQUEST	Уведомление ПК РСЧС о проведении проверки готовности на объекте
SUCCESS	Уведомление ПК РСЧС о завершении проверки готовности на объекте

9.3.5 Примеры сообщений о контрольных проверках приведены в приложении В.

9.3.6 ПК СМИС должен самостоятельно следить за построением цепочки сообщений, относящихся к одному циклу проверки на основе идентификатора сообщения.

9.4 Сообщения о регламентных работах

9.4.1 Сообщения о регламентных работах — класс сообщений, предназначенный для уведомления ПК РСЧС о регламентных работах, происходящих на объекте мониторинга.

Данные сообщения информируют оперативный персонал ОПУ РСЧС о том, что сообщения о различных событиях (происшествиях) (инцидент, авария и т.п.), поступающие от соответствующих объектов мониторинга в период проведения регламентных работ, являются тестовыми и не могут использоваться для принятия решений (реагирования) без специального подтверждения реального факта события со стороны оперативного персонала СМИС объекта.

Структура сообщения о регламентных работах представлена в таблице 10.

Таблица 10 — Структура (описание полей) сообщений класса «Регламентные работы»

Элемент	Тип данных	Обязательное	Описание
MaintenanceId	GUID	Да	Идентификатор регламентных работ
MonitoringObject	Строка	Да/нет	Наименование объекта в ПК РСЧС, содержащееся в идентификационном ключе объекта
MonitoringObjectIdentifier	Строка	Да	Регистрационный номер объекта в ПК РСЧС, содержащийся в идентификационном файле
Note	Строка	Да	Описание проводимых работ, указанное при их начале
Status	Строка	Да	Код текущего состояния работ
FromTime	Дата/время	Да	Время начала работ
PlannedFinishTime	Дата/время	Да	Планируемое время завершения работ, указанное при их начале
FinishTime	Дата/время	Нет	Время завершения работ. Заполняется при завершении
StateCreateTime	Дата/время	Да	Время изменения состояния. Для начала указывается время начала работ
StatePlannedFinishTime	Дата/время	Нет	Планируемое время завершения: - вначале указывается время завершения, указанное при начале работ; - для состояния «TimeExpired» поле не заполняется; - для состояния «Регламентные работы завершены» поле не заполняется
StateFinishTime	Дата/время	Нет	Указывается при завершении работ
StateUser	Строка	Да	Оператор, создавший сообщение о начале работ или изменении состояния
StateNote	Строка	Да	Описание текущего состояния работ

Коды состояний поля Status сообщений о регламентных работах представлены в таблице 11.

Таблица 11 — Коды состояний поля Status сообщений класса «Регламентные работы»

Код	Описание
BeginWork	На объекте начато проведение регламентных работ
TimeExpired	Превышено время проведения регламентных работ
Progress	Изменение времени проведения регламентных работ
Completed	Регламентные работы на объекте завершены

9.4.2 В момент начала регламентных работ ПК СМИС формирует сообщение с кодом «Начало работ», содержащее описание проводимых на объекте работ, а также планируемое время завершения.

9.4.3 Если после начала работ определяется неправильная оценка времени, необходимого для их завершения, ПК СМИС может передать сообщение с кодом «Изменение времени», содержащее новую оценку времени, а также причины, повлекшие за собой это изменение.

9.4.4 ПК СМИС может автоматически следить за временем проведения работ и в случае его превышения передавать в ПК РСЧС сообщение с кодом «Превышение времени».

9.4.5 По окончанию работ ПК СМИС передает сообщение с кодом «Завершение работ».

9.4.6 Примеры сообщений о контрольных проверках приведены в приложении Г.

9.4.7 ПК СМИС должен самостоятельно следить за построением цепочки сообщений, относящихся к одной регламентной работе, на основе идентификатора регламентных работ.

9.5 Проверка подключения

Проверка подключения — класс сообщений, предназначенный для проверки наличия соединения между ПК СМИС и ПК РСЧС. Примеры сообщений приведены в приложении Д.

10 Классификатор событий (происшествий)

10.1 Классификатор событий (происшествий) является описанием списка всех возможных событий (происшествий) для конкретного объекта и экспортируется из ПК СМИС для последующего импорта в ПК РСЧС с целью последующей привязки регламентов действий оперативного персонала ОПУ РСЧС.

10.2 Классификатор событий (происшествий) состоит из следующих элементов: объект мониторинга, событие (происшествие) и регламент [XSD-схема списка событий (происшествий) приведена в приложении Е].

10.2.1 Элемент «Объект мониторинга» содержит описание контролируемых технологических систем и систем инженерно-технического обеспечения объекта. Описание полей элемента приведено в таблице 12.

Таблица 12 — Структура элемента «Объект мониторинга»

Поле	Тип данных	Описание
Name	Строка	Наименование объекта
Identifier	Строка	Уникальный идентификатор объекта в ПК РСЧС
IncidentType	GUID	Идентификатор списка событий

10.2.2 Элемент «Событие (происшествие)» содержит описание событий (происшествий), возможных на объекте мониторинга. Описание полей элемента приведено в таблице 13.

Таблица 13 — Структура элемента «Событие (происшествие)»

Поле	Тип данных	Описание
id	GUID	Идентификатор события (происшествия)
parentId	GUID	Идентификатор родительского события (происшествия) используется для построения иерархических списков
name	Строка	Наименование события (происшествия)
code	Строка	Код события (происшествия) должен быть уникальным для всего списка событий. Присваивается согласно классификатору угроз (см. приложение И)
note	Строка	Примечание
group	Логическое	Признак группы используется для построения иерархических списков

10.2.3 Элемент «Регламент» служит для описания регламента взаимодействия оперативного персонала объекта и ОПУ РСЧС в случае возникновения данного события (происшествия). Описание

действий производится для каждого события (происшествия). Описание полей элемента приведено в таблице 14.

Таблица 14 — Структура элемента «Регламент»

Поле	Тип данных	Описание
content	Строка	Текст регламента
contentType	Строка	Тип данных, записанных в поле content. Поддерживается следующее значение: - text/plain — текст регламента закодирован при помощи base64
status	Строка. Список возможных значений кодов событий представлен в таблице 15	Код события (происшествия), для которого описывается регламент

10.3 Пример классификатора событий (происшествий) и файла, созданного на его основе приведены в приложении Ж.

Таблица 15 — Коды событий для поля Status

Код	Наименование
100	Инцидент
110	Авария
120	Тревога
130	Пожар
200	Снятие с регистрации

10.4 Классификатор угроз СМИС, основанный на классификации ЧС природного и техногенного характера, принятой в РСЧС, представлен в приложении И.

Основой для разработки классификатора событий (происшествий) может служить «Рекомендуемые перечень, кодировка событий (инцидентов, аварий, пожаров, террористических проявлений, ЧС) и состав контролируемых параметров для формирования информационных сообщений в рамках взаимодействия СМИС объектов различного типа и ОПУ РСЧС» (см. приложение К).

Приложение А
(обязательное)

Унифицированная WSDL-схема веб-сервиса программного комплекса систем мониторинга инженерных систем зданий и сооружений и программного комплекса приема информации от систем мониторинга инженерных систем зданий и сооружений объектов органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций

```
<?xml version="1.0" encoding=" WINDOWS-1251"?>
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="gost.e-ecolog.ru
xmlns:tns="gost.e-ecolog.ru "
xmlns:soap="gost.e-ecolog.ru
xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
targetNamespace="http://host:port/monitoring/schemas/node"
name="DispatchServiceImplService">
<wsdl:types>
<xs:schema xmlns:tns="gost.e-ecolog.ru "
targetNamespace="gost.e-ecolog.ru
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="DispatchControlPointRequest">
<xs:complexType>
<xs:sequence>
<xs:element name="Number" type="xs:string"/>
<xs:element name="MonitoringObject" type="xs:string"/>
<xs:element name="MonitoringObjectIdentifier" type="xs:string"/>
<xs:element name="ControlType" type="tns:ControlTypeEnum"/>
<xs:element name="ControlStatus" type="tns:ControlStatusEnum"/>
<xs:element name="RequestTime" type="xs:dateTime"/>
<xs:element name="AcknowledgementTime" type="xs:dateTime" minOccurs="0"/>
<xs:element name="ValidityTime" type="xs:dateTime" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="DispatchControlPointResponse" type="xs:anyType" nillable="true"/>
<xs:element name="DispatchMaintenanceRequest">
<xs:complexType>
<xs:sequence>
<xs:element name="MaintenanceId" type="xs:string"/>
<xs:element name="MonitoringObject" type="xs:string"/>
<xs:element name="MonitoringObjectIdentifier" type="xs:string"/>
<xs:element name="Note" type="xs:string"/>
<xs:element name="Status" type="tns:MaintenanceStatusType"/>
<xs:element name="FromTime" type="xs:dateTime"/>
<xs:element name="PlannedFinishTime" type="xs:dateTime"/>
<xs:element name="FinishTime" type="xs:dateTime" minOccurs="0"/>
<xs:element name="StateCreateTime" type="xs:dateTime"/>
<xs:element name="StatePlannedFinishTime" type="xs:dateTime" minOccurs="0"/>
<xs:element name="StateFinishTime" type="xs:dateTime" minOccurs="0"/>
<xs:element name="StateUser" type="xs:string"/>
<xs:element name="StateNote" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="DispatchMaintenanceResponse">
```

```
<xs:complexType>
<xs:sequence/>
</xs:complexType>
</xs:element>
<xs:element name="DispatchMessageRequest">
<xs:complexType>
<xs:sequence>
<xs:element name="Message" type="tns:NodeMessageType"/>
<xs:element name="Route" type="tns:RouteType"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="DispatchMessageResponse">
<xs:complexType>
<xs:sequence/>
</xs:complexType>
</xs:element>
<xs:element name="Message" type="tns:NodeMessageType"/>
<xs:element name="TestRequest">
<xs:complexType>
<xs:sequence/>
</xs:complexType>
</xs:element>
<xs:element name="TestResponse">
<xs:complexType>
<xs:sequence/>
</xs:complexType>
</xs:element>
<xs:complexType name="NodeMessageType">
<xs:sequence>
<xs:element name="Number" type="xs:string"/>
<xs:element name="Source" type="xs:string" minOccurs="0"/>
<xs:element name="ObjectIdentifier" type="xs:string"/>
<xs:element name="ObjectName" type="xs:string"/>
<xs:element name="IncidentType" type="xs:string"/>
<xs:element name="IncidentTypeName" type="xs:string"/>
<xs:element name="IncidentStatus" type="xs:string"/>
<xs:element name="IncidentStatusName" type="xs:string"/>
<xs:element name="Text" type="xs:string" minOccurs="0"/>
<xs:element name="Time" type="xs:dateTime"/>
<xs:element name="Path" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="RouteType">
<xs:sequence>
<xs:element name="Node" type="tns:NodeType" minOccurs="0"
maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="NodeType">
<xs:sequence>
<xs:element name="SubjectDN" type="xs:string"/>
<xs:element name="ReceiveTime" type="xs:dateTime"/>
<xs:element name="ProcessTime" type="xs:dateTime"/>
</xs:sequence>
</xs:complexType>
<xs:simpleType name="ControlTypeEnum">
<xs:restriction base="xs:string">
<xs:enumeration value="OFFICER"/>
```

<xs:enumeration value="SERVICE"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="ControlStatusEnum">
<xs:restriction base="xs:string">
<xs:enumeration value="REQUEST"/>
<xs:enumeration value="SUCCESS"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="MaintenanceStatusType">
<xs:restriction base="xs:string">
<xs:enumeration value="BeginWork"/>
<xs:enumeration value="Progress"/>
<xs:enumeration value="TimeExpired"/>
<xs:enumeration value="Completed"/>
</xs:restriction>
</xs:simpleType>
<xs:element name="GatewayException" type="tns:GatewayException"/>
<xs:complexType name="GatewayException">
<xs:sequence/>
</xs:complexType>
</xs:schema>
</wsdl:types>
<wsdl:message name="DispatchControlPoint">
<wsdl:part name="DispatchControlPointRequest" element="tns:DispatchControlPointRequest">
</wsdl:part>
</wsdl:message>
<wsdl:message name="DispatchMessageResponse">
<wsdl:part name="DispatchMessageResponse" element="tns:DispatchMessageResponse">
</wsdl:part>
</wsdl:message>
<wsdl:message name="DispatchMessage">
<wsdl:part name="DispatchMessageRequest" element="tns:DispatchMessageRequest">
</wsdl:part>
</wsdl:message>
<wsdl:message name="DispatchControlPointResponse">
<wsdl:part name="DispatchControlPointResponse" element="tns:DispatchControlPointResponse">
</wsdl:part>
</wsdl:message>
<wsdl:message name="GatewayException">
<wsdl:part name="GatewayException" element="tns:GatewayException">
</wsdl:part>
</wsdl:message>
<wsdl:message name="Test">
<wsdl:part name="TestRequest" element="tns:TestRequest"> </wsdl:part>
</wsdl:message>
<wsdl:message name="TestResponse">
<wsdl:part name="TestResponse" element="tns:TestResponse"> </wsdl:part>
</wsdl:message>
<wsdl:message name="DispatchMaintenanceResponse">
<wsdl:part name="DispatchMaintenanceResponse" element="tns:DispatchMaintenanceResponse">
</wsdl:part>
</wsdl:message>
<wsdl:message name="DispatchMaintenance">
<wsdl:part name="DispatchMaintenanceRequest" element="tns:DispatchMaintenanceRequest">
</wsdl:part>
</wsdl:message>
<wsdl:portType name="DispatchService">
<wsdl:operation name="DispatchControlPoint">

```
<wsdl:input name="DispatchControlPoint" message="tns:DispatchControlPoint">
</wsdl:input>
<wsdl:output name="DispatchControlPointResponse"
message="tns:DispatchControlPointResponse">
</wsdl:output>
<wsdl:fault name="GatewayException" message="tns:GatewayException">
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="Test">
<wsdl:input name="Test" message="tns:Test">
</wsdl:input>
<wsdl:output name="TestResponse" message="tns:TestResponse">
</wsdl:output>
<wsdl:fault name="GatewayException" message="tns:GatewayException">
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="DispatchMessage">
<wsdl:input name="DispatchMessage" message="tns:DispatchMessage">
</wsdl:input>
<wsdl:output name="DispatchMessageResponse"
message="tns:DispatchMessageResponse"> </wsdl:output>
<wsdl:fault name="GatewayException" message="tns:GatewayException">
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="DispatchMaintenance">
<wsdl:input name="DispatchMaintenance"
message="tns:DispatchMaintenance">
</wsdl:input>
<wsdl:output name="DispatchMaintenanceResponse"
message="tns:DispatchMaintenanceResponse">
</wsdl:output>
<wsdl:fault name="GatewayException"
message="tns:GatewayException">
</wsdl:fault>
</wsdl:operation>
</wsdl:portType>
<wsdl:binding name="DispatchServiceImplServiceSoapBinding"
type="tns:DispatchService">
<soap:binding transport="gost.e-ecolog.ru                    " style="document"/>
<wsdl:operation name="DispatchControlPoint">
<soap:operation style="document" soapAction=""/>
<wsdl:input name="DispatchControlPoint">
<soap:body use="literal"/>
</wsdl:input>
<wsdl:output name="DispatchControlPointResponse">
<soap:body use="literal"/>
</wsdl:output>
<wsdl:fault name="GatewayException">
<soap:fault name="GatewayException" use="literal"/>
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="Test">
<soap:operation style="document" soapAction=""/>
<wsdl:input name="Test">
<soap:body use="literal"/>
</wsdl:input>
<wsdl:output name="TestResponse">
<soap:body use="literal"/>
</wsdl:output>
```

```
<wsdl:fault name="GatewayException">
<soap:fault name="GatewayException" use="literal"/>
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="DispatchMessage">
<soap:operation style="document" soapAction=""/>
<wsdl:input name="DispatchMessage">
<soap:body use="literal"/>
</wsdl:input>
<wsdl:output name="DispatchMessageResponse">
<soap:body use="literal"/>
</wsdl:output>
<wsdl:fault name="GatewayException">
<soap:fault name="GatewayException" use="literal"/>
</wsdl:fault>
</wsdl:operation>
<wsdl:operation name="DispatchMaintenance">
<soap:operation style="document" soapAction=""/>
<wsdl:input name="DispatchMaintenance">
<soap:body use="literal"/>
</wsdl:input>
<wsdl:output name="DispatchMaintenanceResponse">
<soap:body use="literal"/>
</wsdl:output>
<wsdl:fault name="GatewayException">
<soap:fault name="GatewayException" use="literal"/>
</wsdl:fault>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="DispatchServiceImplService">
<wsdl:port name="DispatchServicePort"
binding="tns:DispatchServiceImplServiceSoapBinding">
<soap:address location="gost.e-ecolog.ru                    >
</wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

Приложение Б
(справочное)

Примеры сообщений о событиях (происшествиях), происходящих на объекте мониторинга

Инцидент

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="http://host:port/monitoring/schemas/node">
<Message>
<Number>3b58e66e-ffbb-40fa-8571-4d60662130a1</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>1.1.1.4</IncidentType>
<IncidentTypeName>Инцидент в технологической системе объекта</IncidentTypeName>
<IncidentStatus>100</IncidentStatus>
<IncidentStatusName>INCIDENT</IncidentStatusName>
<Text>Уровни в емкостях пожароопасных продуктов вышли за предупредительные уставки</Text>
<Time>2017-11-20T08:00:00.000+04:00</Time>
<Path>Цех № K, Установка № L</Path>
</Message>
</DispatchMessageRequest>
```

Авария

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="http://host:port/monitoring/schemas/node">
<Message>
<Number>d1d05e81-cbab-418b-853b-1633124cda8d</Number>
<Source>3b58e66e-ffbb-40fa-8571-4d60662130a1</Source>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>1.1.2.2</IncidentType>
<IncidentTypeName>Авария в технологической системе объекта</IncidentTypeName>
<IncidentStatus>110</IncidentStatus>
<IncidentStatusName>DAMAGE</IncidentStatusName>
<Text>Параметры концентраций вредных веществ в производственных помещениях и рабочей зоне открытых установок (ПДК) вышли за аварийные уставки</Text>
<Time>2017-11-20T08:05:00.000+04:00</Time>
<Path> Цех № K, Установка № L</Path>
</Message>
</DispatchMessageRequest>
```

Снятие с регистрации

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="gost.e-ecolog.ru                    ">
<Message>
<Number> 9832af13-054e-414c-8e5f-650c9c2abd63</Number>
<Source> d1d05e81-cbab-418b-853b-1633124cda8d</Source>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>1.1.2.2</IncidentType>
<IncidentTypeName>Снятие с регистрации события в технологической системе объекта</IncidentTypeName>
<IncidentStatus>200</IncidentStatus>
<IncidentStatusName>SAFETY</IncidentStatusName>
<Text>Устранение инцидента в технологической системе</Text>
<Time>2017-11-20T08:10:00.000+04:00</Time>
<Path>Цех № K, Установка № L</Path>
</Message>
</DispatchMessageRequest>
```

Тревога

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="http://host:port/monitoring/schemas/node">
<Message>
<Number> 6b228795-bdc3-4696-845a-febd7fab67a0</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>3.1.2</IncidentType>
<IncidentTypeName>Возможные террористические проявления</IncidentTypeName>
<IncidentStatus>120</IncidentStatus>
<IncidentStatusName>ALERT</IncidentStatusName>
<Text>Несанкционированное проникновение на объект</Text>
<Time>2017-11-20T08:15:00.000+04:00</Time>
<Path>Пост № К</Path>
</Message>
</DispatchMessageRequest>
```

Пожар

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="gost.e-ecolog.ru >
<Message>
<Number> aaf993a8-a54c-41a6-a4fb-60a0227f60b2</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>1.1.1.1</IncidentType>
<IncidentTypeName>Пожар/взрыв (с возможным последующим горением) в зданиях, на коммуникациях и технологическом оборудовании промышленных объектов</IncidentTypeName>
<IncidentStatus>130</IncidentStatus>
<IncidentStatusName>FIRE</IncidentStatusName>
<Text>Пожар на технологическом оборудовании объекта мониторинга</Text>
<Time>2017-11-20T08:20:00.000+04:00</Time>
<Path> Цех № К, Установка № </Path>
</Message>
</DispatchMessageRequest>
```

Авария — сообщение, формируемое оперативным персоналом по факту аварии

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMessageRequest xmlns="gost.e-ecolog.ru >
<Message>
<Number> 5e31317a-e502-4d4d-83a4-db5986e5c697</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>DAMAGE</IncidentType>
<IncidentTypeName>Обобщенный сигнал «Авария»</IncidentTypeName>
<IncidentStatus>111</IncidentStatus>
<IncidentStatusName>DAMAGE</IncidentStatusName>
<Text>Обобщенный сигнал «Авария в технологических процессах объекта, формируемый оперативным персоналом»</Text>
<Time>2017-11-20T08:25:00.000+04:00</Time>
</Message>
</DispatchMessageRequest>
```

Тревога — сигнал, формируемый оперативным персоналом (от тревожной кнопки)

```
<DispatchMessageRequest xmlns="http://host:port/monitoring/schemas/node">
<Message>
<Number> 83441dca-bdca-46f1-8836-4c8ba5227d03</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>ALERT</IncidentType>
<IncidentTypeName>Тревога </IncidentTypeName>
<IncidentStatus>121</IncidentStatus>
<IncidentStatusName>ALERT</IncidentStatusName>
<Text>Сигнал «Тревога на объекте», формируемый оперативным персоналом</Text>
<Time>2017-11-20T08:30:00.000+04:00</Time>
</Message>
</DispatchMessageRequest>
```

Пожар — сообщение, формируемое оперативным персоналом по факту события

```
<DispatchMessageRequest xmlns="gost.e-ecolog.ru                    >
<Message>
<Number> 3cca9e8e-b908-426b-9b37-5e523195f182</Number>
<ObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</ObjectIdentifier>
<ObjectName>Объект мониторинга</ObjectName>
<IncidentType>FIRE</IncidentType>
<IncidentTypeName>Пожар на объекте</IncidentTypeName>
<IncidentStatus>131</IncidentStatus>
<IncidentStatusName>FIRE</IncidentStatusName>
<Text>Сигнал «Пожар на объекте», формируемый оперативным персоналом</Text>
<Time>2017-11-20T08:35:00.000+04:00</Time>
</Message>
</DispatchMessageRequest>
```

Ответ ПК РСЧС

```
<?xml version=»1.0» encoding=»WINDOWS-1251»?>
<DispatchMessageResponse xmlns=»gost.e-ecolog.ru                    >
```

Приложение В
(справочное)

Примеры сообщений о проведении проверки готовности оперативного персонала и программного комплекса системы мониторинга инженерных систем зданий и сооружений

Запрос готовности оперативного персонала СМИС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchControlPointRequest xmlns="gost.e-ecolog.ru                    ">
<Number>4cbfc495-ab89-4ac8-8cd3-71144a7c5f03</Number>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<ControlType>OFFICER</ControlType>
<ControlStatus>REQUEST</ControlStatus>
<RequestTime>2017-11-20T08:00:00.000+04:00</RequestTime>
</DispatchControlPointRequest>
```

Подтверждение готовности оперативного персонала СМИС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchControlPointRequest xmlns="http://host:port/monitoring/schemas/node">
<Number>4cbfc495-ab89-4ac8-8cd3-71144a7c5f03</Number>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<ControlType>OFFICER</ControlType>
<ControlStatus>SUCCESS</ControlStatus>
<RequestTime>2017-11-20T08:00:00.000+04:00</RequestTime>
<AcknowledgementTime>2017-11-20T08:01:00.000+04:00</AcknowledgementTime>
<ValidityTime>2017-11-20T08:30:00.000+04:00</ValidityTime>
</DispatchControlPointRequest>
```

Запрос готовности ПК СМИС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchControlPointRequest xmlns="gost.e-ecolog.ru                    ">
<Number>215fc9d3-0fe2-4602-84d0-b5ac47ca1fed</Number>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<ControlType>SERVICE</ControlType>
<ControlStatus>REQUEST</ControlStatus>
<RequestTime>2017-11-20T08:05:00.000+04:00</RequestTime>
</DispatchControlPointRequest>
```

Подтверждение готовности ПК СМИС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchControlPointRequest xmlns="gost.e-ecolog.ru                    ">
<Number>215fc9d3-0fe2-4602-84d0-b5ac47ca1fed</Number>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<ControlType>SERVICE</ControlType>
<ControlStatus>SUCCESS</ControlStatus>
<RequestTime>2017-11-20T08:05:00.000+04:00</RequestTime>
<AcknowledgementTime>2017-11-20T08:11:00.000+04:00</AcknowledgementTime>
<ValidityTime>2017-11-20T08:35:00.000+04:00</ValidityTime>
</DispatchControlPointRequest>
```

Ответ ПК РСЧС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchControlPointResponse xmlns="http://host:port/monitoring/schemas/node"/>
```

Приложение Г
(справочное)

Примеры сообщений о проведении регламентных работ на объекте мониторинга

Начало работ

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMaintenanceRequest xmlns="http://host:port/monitoring/schemas/node">
<MaintenanceId>b10d1d33-e7d8-427c-b912-c1d1143a8713</MaintenanceId>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<Note>Проведение регламентных работ в системе электроснабжения</Note>
<Status>BEGINWORK</Status>
<FromTime>2017-11-20T08:00:00.000+04:00</FromTime>
<PlannedFinishTime>2017-11-20T09:00:00.000+04:00</PlannedFinishTime>
<StateCreateTime>2017-11-20T08:00:00.000+04:00</StateCreateTime>
<StatePlannedFinishTime>2017-11-20T09:00:00.000+04:00</StatePlannedFinishTime>
<StateUser>Собакин С.О.</StateUser>
<StateNote>Начало проведение регламентных работ</StateNote>
</DispatchMaintenanceRequest>
```

Превышение времени регламентных работ

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMaintenanceRequest xmlns="gost.e-ecolog.ru                    ">
<MaintenanceId>b10d1d33-e7d8-427c-b912-c1d1143a8713</MaintenanceId>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<Note>Проведение регламентных работ в системе электроснабжения</Note>
<Status>TIMEEXPIRED</Status>
<FromTime>2017-11-20T08:00:00.000+04:00</FromTime>
<PlannedFinishTime>2017-11-20T09:00:00.000+04:00</PlannedFinishTime>
<StateCreateTime>2017-11-20T09:01:00.000+04:00</StateCreateTime>
<StateUser>Собакин С.О.</StateUser>
<StateNote>Превышено время проведения регламентных работ</StateNote>
</DispatchMaintenanceRequest>
```

Изменение времени регламентных работ

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMaintenanceRequest xmlns="http://host:port/monitoring/schemas/node">
<MaintenanceId>b10d1d33-e7d8-427c-b912-c1d1143a8713</MaintenanceId>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<Note>Проведение регламентных работ в системе электроснабжения</Note>
<Status>PROGRESS</Status>
<FromTime>2017-11-20T08:00:00.000+04:00</FromTime>
<PlannedFinishTime>2017-11-20T09:00:00.000+04:00</PlannedFinishTime>
<StateCreateTime>2017-11-20T09:02:00.000+04:00</StateCreateTime>
<StatePlannedFinishTime>2017-11-20T10:00:00.000+04:00</StatePlannedFinishTime>
<StateUser>Курицин С.М.</StateUser>
<StateNote>Изменение времени проведения регламентных работ</StateNote>
</DispatchMaintenanceRequest>
```

Завершение регламентных работ

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMaintenanceRequest xmlns="gost.e-ecolog.ru                    >
<MaintenanceId>b10d1d33-e7d8-427c-b912-c1d1143a8713</MaintenanceId>
<MonitoringObject>Объект мониторинга</MonitoringObject>
<MonitoringObjectIdentifier>1c04fd70-5359-40de-a1cb-cf86616a333b</MonitoringObjectIdentifier>
<Note>Проведение регламентных работ в системе электроснабжения</Note>
<Status>COMPLETED</Status>
<FromTime>2017-11-20T08:00:00.000+04:00</FromTime>
<PlannedFinishTime>2017-11-20T09:00:00.000+04:00</PlannedFinishTime>
<FinishTime>2017-11-20T10:00:00.000+04:00</FinishTime>
<StateCreateTime>2017-11-20T10:00:00.000+04:00</StateCreateTime>
<StateFinishTime>2017-11-20T10:00:00.000+04:00</StateFinishTime>
<StateUser>Пельменев И.В.</StateUser>
<StateNote>Регламентные работы завершены</StateNote>
</DispatchMaintenanceRequest>
```

Ответ ПК РСЧС

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<DispatchMaintenanceResponse xmlns="gost.e-ecolog.ru                    >
```

Приложение Д
(справочное)

Примеры сообщений о проверке соединения между программным комплексом системы мониторинга инженерных систем зданий и сооружений и программным комплексом приема информации от систем мониторинга инженерных систем зданий и сооружений объектов органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций

Сообщение, используемое для проверки подключения

```
<?xml version="1.0" encoding="UTF-8"?>
<TestRequest xmlns="gost.e-ecolog.ru                    >
```

Ответ ПК РСЧС при наличии подключения

```
<?xml version="1.0" encoding="UTF-8"?>
<TestResponse xmlns="gost.e-ecolog.ru                    >
```

Приложение Е
(справочное)

XSD-схема списка событий (происшествий)

```
<?xml version="1.0" encoding=" WINDOWS-1251"?>
<xsd:schema xmlns:xsd="gost.e-ecolog.ru
elementFormDefault="qualified" attributeFormDefault="qualified">
<xsd:element name="MonitoringObject" type="MonitoringObjectType">
<xsd:unique name="UniqueIncidentTypeCode">
<xsd:selector xpath="IncidentType"/>
<xsd:field xpath="Code"/>
</xsd:unique>
</xsd:element>
<xsd:complexType name="MonitoringObjectType">
<xsd:sequence>
<xsd:element name="Name" type="xsd:string" minOccurs="1" maxOccurs="1">
<xsd:annotation>
<xsd:documentation> Наименование объекта </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Identifier" type="xsd:string" minOccurs="1" maxOccurs="1">
<xsd:annotation>
<xsd:documentation> Идентификатор объекта в системе </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="IncidentType" minOccurs="0" maxOccurs="unbounded">
<xsd:complexType>
<xsd:sequence>
<xsd:element name="Id" type="GuidType">
<xsd:annotation>
<xsd:documentation> Идентификатор списка событий
(происшествий)</xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="ParentId" type="GuidType" minOccurs="0">
<xsd:annotation>
<xsd:documentation> Идентификатор родительского события </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Name" type="xsd:string">
<xsd:annotation>
<xsd:documentation> Наименование списка событий (происшествий)
</xsd:element>
<xsd:element name="Code" type="xsd:string">
<xsd:annotation>
<xsd:documentation> Код события (происшествия)</xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Note" type="xsd:string" minOccurs="0">
<xsd:annotation>
<xsd:documentation> Примечание к списку событий</xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Group" type="xsd:boolean">
<xsd:annotation>
<xsd:documentation> Признак группы </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Guidelines">
```

```
<xsd:complexType>
<xsd:sequence>
<xsd:element name="Guideline" type="GuidelineType" minOccurs="0" maxOccurs="unbounded">
</xsd:element>
</xd:sequence>
</xsd:complexType>
<xsd:unique name="UniqueIncidentTypeGuideline">
<xsd:selector xpath="Guideline"/>
<xsd:field xpath="Status"/>
</xsd:unique>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsdsequence>
</xsd:complexType>
<xsd:complexType name="GuidelineType">
<xsd:sequence>
<xsd:element name="Content" type="xsd:base64Binary" minOccurs="1" maxOccurs="1">
<xsd:annotation>
<xsd:documentation> Текст регламента (в кодировке Base64) </xsd:documentation>
</xsd:anotation>
</xsd:element>
<xsd:element name="ContentType" type="ContentTypeEnum" minOccurs="1"
maxOccurs="1">
<xsd:annotation>
<xsd:documentation> Тип данных (text/plain) </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Status" type="IncidentStatusEnum" minOccurs="1" maxOccurs="1">
<xsd:annotation>
<xsd:documentation> Код статуса события </xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="IncidentStatusEnum">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="100"/>
<xsd:enumeration value="110"/>
<xsd:enumeration value="111"/>
<xsd:enumeration value="120"/>
<xsd:enumeration value="121"/>
<xsd:enumeration value="130"/>
<xsd:enumeration value="131"/>
<xsd:enumeration value="200"/>
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="ContentTypeEnum">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="text/plain"/>
</xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="GuidType">
<xsd:restriction base="xsd:string">
<xsd:pattern value="[0-9,A-F,a-f]{8}-[0-9,A-F,a-f]{4}-[0-9,A-F,a-f]{4}-[0-9,A-F,a-f]{4}-[0-9,A-F,a- f]{12}"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:schema>
```

Приложение Ж
(справочное)

Пример списка событий (происшествий)

В приложении Ж представлен пример списка событий (происшествий) (см. таблицу Ж.1) и пример файла списка событий (происшествий)

Таблица Ж.1 — Пример списка событий (происшествий)

Объект мониторинга	Описание событий на объекте	Регламент действий оперативного персонала СМИС
1 Технологические системы объекта 1.1 Цех №, установка №	Инцидент	Выяснить причину инцидента, контролировать развитие ситуации
.....		
2 Системы инженерно-технического обеспечения 2.1 Система электроснабжения 2.2 Система теплоснабжения	Авария Тревога	Выяснить причину аварии, оповестить оперативного дежурного и действовать согласно плану ликвидации аварийных событий Проверить, оповестить службы безопасности, действовать по плану в случае террористической угрозы
.....		
3 Системы противопожарной защиты 3.1 Автоматические системы пожарной сигнализации 3.2 Автоматические установки пожаротушений 3.3 Системы оповещения и управления эвакуацией	Пожар Снятие с регистрации	Проверить, вызвать пожарных, оповестить оперативного дежурного, действовать по плану при пожаре
.....		
4 Системы связи и оповещения 4.1 Система телефонной связи		
.....		
5 Системы безопасности 5.1 Система контроля и управления доступом		
.....		
6 Система мониторинга строительных (несущих) конструкций и оснований зданий и сооружений		

Пример файла списка событий (происшествий)

```
Пример файла списка событий (происшествий)
<?xml version="1.0" encoding=" WINDOWS-1251"?>
<MonitoringObject>
<Name> Объект мониторинга </Name>
<Identifier>1c04fd70-5359-40de-a1cb-cf86616a333b</Identifier>

<IncidentType>
<Id>8d81f447-7de5-4b5a-af85-10dc138fbe78</Id>
<Name>Техногенные угрозы. Чрезвычайные ситуации техногенного характера на объекте</Name>
<Code>1.1</Code>
<Group>true</Group>
<Guidelines/>
</IncidentType>

<IncidentType>
<Id>472135ba-569e-49d0-8e41-707470e7655c</Id>
<ParentId>8d81f447-7de5-4b5a-af85-10dc138fbe78</ParentId>
<Name>Аварии в технологических системах. Цех № N, установка № L </Name>
```

<Code>1.1.12.1</Code>
<Guidelines>
<Guideline>
<Content>
wvv/8e3o8vwg7/Do9+jt8yDu8urr/vfl7ej/lP3r5ery8O7x7eDh5uXt6P8g7uH65ery4A==
</Content>
<ContentType>text/plain</ContentType>
<Status>100</Status>
</Guideline>
<Guideline>
<Content>
MS4gzu/u4uXx8ujy/CDu7+Xw4PLo4u3u4+4g5OXm8/Dt7uPuDQoyLiDH4OTl6fHy4u7i4PL8IPDl5+Xw4u375SDo8fLu9+
+3o6ugg/evl6vLw7vHt4OHm5e3o/w0K
</Content>
<ContentType>text/plain</ContentType>
<Status>110</Status>
</Guideline>
</Guidelines>
</IncidentType>

<IncidentType>
<Id>1790cb87-0208-4dd1-b7a7-bc766169329e</Id>
<ParentId>8d81f447-7de5-4b5a-af85-10dc138fbe78</ParentId>
<Name>Аварии в системах инженерно-технического обеспечения. Система электроснабжения</Name>
<Code>1.1.12.2</Code>
<Guidelines>
<Guideline>
<Content>
wvv/8e3o8vwg7/Do9+jt8yDu8urr/vfl7ej/lODi4PDo6e3u4+4g7vHi5fnl7ej/lO7h+uXq8uA=
</Content>
<ContentType>text/plain</ContentType>
<Status>100</Status>
</Guideline>
<Guideline>
<Content>
wvvn4uDy/CDw5ezu7fLt8/4g4fDo4+Dk8w==
</Content>
<ContentType>text/plain</ContentType>
<Status>110</Status>
</Guideline>
</Guidelines>
</IncidentType>

<IncidentType>
<Id>ff6aab35-3e73-450d-8df4-1fcbe0a3c152</Id>
<ParentId>8d81f447-7de5-4b5a-af85-10dc138fbe78</ParentId>
<Name>Аварии в системах инженерно-технического обеспечения. Система теплоснабжения</Name>
<Code>1.1.12.2</Code>
<Guidelines>
<Guideline>
<Content>
wvv/8e3o8vwg7/Do9+jt8yDu8urr/vfl7ej/lPLl7+vu8e3g4ebl7ej/lO7h+uXq8uA=
</Content>
<ContentType>text/plain</ContentType>
<Status>100</Status>
</Guideline>
<Guideline>
<Content>

```
wvvn4uDy/CDw5ezu7fLt8/4g4fDo4+Dk8w==
</Content>
<ContentType>text/plain</ContentType>
<Status>110</Status>
</Guideline>
</Guidelines>
</IncidentType>
.....
</MonitoringObject>
```

Приложение И
(обязательное)

Классификатор угроз системы мониторинга инженерных систем зданий и сооружений объектов

Классификатор угроз СМИС основан на классификации ЧС природного и техногенного характера, принятой в РСЧС в соответствии с [6], [7], [8], [9] (см. таблицу И.1)

Таблица И.1 — Классификатор угроз СМИС

Тип угрозы Z	Класс угрозы K	Вид, подвид угрозы V
1 Техногенные угрозы	1 Чрезвычайные ситуации техногенного характера: - на объекте; - на прилегающих соседних объектах и территориях, потенциально опасные для объекта (внешние)	1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 1.2 Пожары (взрывы) на объектах добычи, переработки и хранения легковоспламеняющихся, горючих и взрывчатых веществ 1.3 Пожары (взрывы) на транспорте 1.4 Пожары (взрывы) в шахтах, подземных выработках, метрополитенах 1.5 Пожары (взрывы) в зданиях и сооружениях жилого, социально-бытового, культурного назначения 1.6 Обнаружение неразорвавшихся боеприпасов 1.7 Обнаружение, утрата взрывчатых веществ (боеприпасов) 1.8 Пожары (взрывы) на магистральных газо-, нефте-, продуктопроводах
		2 Аварии с выбросом (угрозой выброса) опасных веществ 2.1 Аварии с выбросом (угрозой выброса) аварийно химически опасных веществ (АХОВ) при их производстве, переработке или хранении (захоронении) 2.2 Аварии на транспорте с выбросом (угрозой выброса) АХОВ 2.3 Образование и распространение АХОВ в процессе химических реакций, начавшихся в результате аварии 2.4 Обнаружение(утрата) источников АХОВ 2.5 Внезапные выбросы метана, углекислого газа и других ядовитых веществ и газов 2.6 Выбросы на нефтяных и газовых месторождениях (открытые фонтаны нефти и газа)
		3 Аварии с массовым выбросом загрязняющих веществ 3.1 Аварии на коммунальных системах жизнеобеспечения (на канализационных системах с массовым выбросом загрязняющих веществ; в системах снабжения населения питьевой водой; на тепловых сетях в холодное время года; на коммунальных газопроводах) 3.2 Аварии на очистных сооружениях с массовым выбросом загрязняющих веществ (сточных вод промышленных предприятий), промышленных установках по очистке газов
		4 Аварии с выбросом (угрозой выброса) радиоактивных веществ 4.1 Аварии на атомных электростанциях, промышленных и исследовательских ядерных установках с выбросом (угрозой выброса) радиоактивных веществ (РВ) 4.2 Аварии с выбросом (угрозой выброса) РВ на предприятиях ядерно-топливного цикла

Продолжение таблицы И.1

Тип угрозы Z	Класс угрозы K	Вид, подвид угрозы V
		4.3 Аварии транспортных средств и космических аппаратов с ядерными установками или грузом РВ на борту 4.4 Аварии на пунктах хранения ядерных материалов и радиоактивных веществ, хранилищах отработавшего ядерного топлива, пунктах хранения или захоронения радиоактивных отходов 4.5 Обнаружение (утрата) источников ионизирующих излучений
		5 Аварии с выбросом (угрозой выброса) опасных биологических веществ (ОБВ) 5.1 Аварии с выбросом (угрозой выброса) ОБВ на предприятиях и в научно-исследовательских учреждениях (лабораториях) 5.2 Аварии на транспорте с выбросом (угрозой выброса) ОБВ 5.3 Обнаружение (утрата) ОБВ
		6 Внезапное обрушение зданий, сооружений, пород 6.1 Обрушение элементов транспортных коммуникаций 6.2 Обрушение производственных зданий и сооружений 6.3 Обрушение зданий и сооружений жилого, социально-бытового и культурного назначения 6.4 Обрушение пород и полезных ископаемых в горных выработках, включая карьеры 6.5 Авария на подземном сооружении
		7 Транспортные аварии (катастрофы) 7.1 Аварии грузовых поездов 7.2 Авиационные катастрофы в населенных пунктах 7.3 Аварии (катастрофы) на автодорогах 7.4 Аварии транспорта на мостах, в тоннелях, на ж/д переездах
		8 Аварии на электроэнергетических системах 8.1 Аварии на автономных электростанциях с долговременным перерывом электроснабжения потребителей 8.2 Аварии на электроэнергетических системах (сетях) с долговременным перерывом электроснабжения основных потребителей и обширных территорий 8.3 Выход из строя транспортных электрических контактных сетей
		9 Аварии на коммунальных системах жизнеобеспечения 9.1 Аварии на канализационных системах с массовым выбросом загрязняющих веществ 9.2 Аварии в системах снабжения населения питьевой водой 9.3 Аварии на тепловых сетях (системах горячего водоснабжения) в холодное время года 9.4 Аварии на коммунальных газопроводах
		10 Аварии на очистных сооружениях 10.1 Аварии на очистных сооружениях сточных вод промышленных предприятий с массовым выбросом загрязняющих веществ 10.2 Аварии на промышленных установках по очистке газов (массовый выброс загрязняющих веществ)

Окончание таблицы И.1

Тип угрозы Z	Класс угрозы K	Вид, подвид угрозы V
		11 Гидродинамические аварии 11.1 Прорывы плотин (дамб, шлюзов, перемычек и др.) с образованием волн прорыва и катастрофических затоплений 11.2 Прорывы плотин (дамб, шлюзов, перемычек и др.) с образованием прорывного паводка 11.3 Прорывы плывунов, пульпы и глинистой массы, а также затопление водой действующих горных выработок при разработке полезных ископаемых 11.4 Размыв береговой полосы штормовыми нагонами
		12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
2 Природные угрозы	2 Природные чрезвычайные ситуации, потенциально опасные для объекта (внешние)	1 Опасные геофизические явления (землетрясения, извержения вулканов)
		2 Опасные геологические явления (оползни, сели, обвалы, склоновый смыв, просадка лессовых пород, карстовая просадка, повышение уровня грунтовых вод)
		3 Опасные метеорологические явления (бури, ураганы, смерчи, шквалы, крупный град, сильный дождь, сильный снегопад, сильный гололед, сильный мороз, сильная жара, лавины…)
		4 Морские опасные гидрологические явления (тайфуны, цунами)
		5 Опасные гидрологические явления (наводнения, половодье, дождевые паводки, заторы, ветровые нагоны)
		6 Природные пожары (лесные, степные, торфяные)
3 Биолого-социальные угрозы	Биолого-социальные чрезвычайные ситуации по факту	1 Террористические проявления: 1.1 Без определения — сигнал от кнопки «Тревога» 1.2 Несанкционированное проникновение на объект 1.3 Угроза взрыва 1.4 Угроза газовой атаки 1.5 Взрыв 1.6 Давка (скопление людей) 1.7 Захват заложников 1.8 Массовая драка 1.9 Нападение 1.10 Нарушение общественного порядка 1.11 Обнаружение взрывоопасных предметов 1.12 Обнаружение оружия 1.13 Отравления 1.14 Применение газового оружия 1.15 Применение огнестрельного оружия 1.16 Применение холодного оружия 1.17 Авария на опасном производстве, вызванная террористическим актом 1.18 Обнаружение источников ионизирующего излучения
		2 Единичные случаи экзотических и особо опасных инфекционных заболеваний
		3 Групповые случаи опасных инфекционных заболеваний

Приложение К
(рекомендуемое)

Рекомендуемые перечень, кодировка событий (инцидентов, аварий, пожаров, террористических проявлений, чрезвычайных ситуаций) и состав контролируемых параметров для формирования информационных сообщений в рамках взаимодействия систем мониторинга инженерных систем зданий и сооружений объектов различного типа и органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций

В приложении К представлены рекомендуемые перечень, состав контролируемых СМИС факторов (параметров) и кодировка событий (происшествий) для формирования сообщений СМИС в рамках информационного взаимодействия СМИС объектов различной ведомственной принадлежности и функционального предназначения с ОПУ РСЧС (см. таблицу К.1).

Таблица К.1 — Рекомендуемые перечень, кодировка событий (инцидентов, аварий, пожаров, террористических проявлений, чрезвычайных ситуаций) и состав контролируемых параметров для формирования информационных сообщений в рамках взаимодействия СМИС объектов различного типа и ОПУ РСЧС

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС. Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС. Код события
Технологические системы ОПО, ГТС, ОИАЭ Сигналы ПК СМИС: - «Авария/инцидент» в технологических процессах; - «Пожар»; - «Тревога»; - обобщенный сигнал «Авария», формируемый оперативным персоналом по факту аварии; - обобщенный сигнал «Тревога», формируемый оперативным персоналом по факту (от тревожной кнопки); - обобщенный сигнал «Пожар», формируемый оперативным персоналом по факту пожара. Примечания 1 Сигналы «Авария/инцидент», «Пожар», «Тревога» формируются в автоматизированном режиме ПК СМИС. 2 Обобщенные сигналы «Авария», «Пожар», «Тревога» формируются по факту оперативным персоналом СМИС.	ОПО нефте- и газодобычи, нефтепереработки, нефтехимии Состояние технологических систем (цех №, установка №): - сообщение об аварии/инциденте (устранении инцидента) в технологической системе — параметр(ы) процесса, вышедший(ие)/вернувшийся(еся) за аварийные/предупредительные уставки: параметры вибрации, сдвига, зазоров, частоты вращения оборудования, параметры концентраций, расхода, температуры и давления в установке, уровни в емкостях пожароопасных и вредных продуктов, уровни в дренажных емкостях, приямках и канализационных колодцах, параметры электроснабжения, тепло-, водо- и топливоснабжения оборудования, давления воздуха контрольно-измерительных приборов и аппаратуры; - нарушения требований нормативных правовых актов Российской Федерации, а также нормативных технических документов, устанавливающих правила ведения работ на ОПО: параметры пожаро- и газоопасности,	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 1.2 Пожары (взрывы) на объектах добычи, переработки и хранения легковоспламеняющихся, горючих и взрывчатых веществ 1.8 Пожары (взрывы) на магистральных газо-, нефте-, продуктопроводах 2 Аварии с выбросом (угрозой выброса) опасных веществ 2.1 Аварии с выбросом (угрозой выброса) АХОВ при их производстве, переработке или хранении (захоронении) 2.3 Образование и распространение АХОВ в процессе химических реакций, начавшихся в результате аварии 2.5 Внезапные выбросы метана, углекислого газа и других ядовитых веществ и газов 2.6 Выбросы на нефтяных и газовых месторождениях (открытые фонтаны нефти и газа)

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
3 Конкретный состав и параметры событий (аварий и инцидентов), включаемые в классификатор, формируются на стадиях разработки технического задания на проектирование СМИС с учетом ведомственных нормативно-технических и руководящих документов по прогнозированию аварий, предупреждению ЧС и обмену информацией в области защиты населения и территорий от ЧС Код состояния (статуса) события: 100 — инцидент; 110 — авария; 120 — тревога; 130 — пожар; 200 — снятие с регистрации; 111 — обобщенный сигнал «Авария», формируемый оперативным персоналом по факту аварии; 121 — обобщенный сигнал «Тревога», формируемый оперативным персоналом по факту нажатия тревожной кнопки; 131 — обобщенный сигнал «Пожар», формируемый оперативным персоналом по факту пожара	параметры концентрации вредных веществ в производственных помещениях и рабочей зоне открытых установок, - срабатывание предохранительных клапанов, мембранных устройств; - отказ или повреждение деталей и узлов технических устройств, разгерметизация насосного оборудования Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	3 Аварии с массовым выбросом загрязняющих веществ 3.2 Аварии на очистных сооружениях с массовым выбросом загрязняющих веществ (сточных вод промышленных предприятий), промышленных установках по очистке газов 6 Внезапное обрушение зданий и сооружений 6.1 Внезапное обрушение производственных зданий и сооружений 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 1.1 Аварии в технологических системах 1.2 Аварии в системах инженерно-технического обеспечения
	ОПО металлургии Состояние технологических систем (цех №, установка №): - сообщение об аварии/инциденте (устранении инцидента) в технологической системе — параметр(ы) процесса, вышедший(ие)/вернувшийся(еся) за аварийные/предупредительные уставки: параметры расхода, температуры, давления и температуры в газоиспользующих установках, в системах оборотного водоснабжения и охлаждения, уровни в дренажных емкостях, приямках и канализационных колодцах, параметры энергоносителей (электроснабжения; температуры, давления и расхода оборотной воды системы охлаждения); - нарушения требований нормативных правовых актов Российской Федерации, а также нормативных технических документов, устанавливающих правила ведения работ на ОПО: параметры довзрывных концентраций в воздухе рабочей зоны производственных помещений (паров CH_4),	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 2 Аварии с выбросом (угрозой выброса) опасных веществ 2.1 Аварии с выбросом (угрозой выброса) аварийно химически опасных веществ (АХОВ) при их производстве, переработке или хранении (захоронении) 2.5 Внезапные выбросы метана, углекислого газа и других ядовитых веществ и газов 3 Аварии с массовым выбросом загрязняющих веществ 3.2 Аварии на очистных сооружениях с массовым выбросом загрязняющих веществ (сточных вод промышленных предприятий), на промышленных установках по очистке газов

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов. Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	параметры концентрации вредных веществ в производственных помещениях и рабочей зоне (пыли, СО); - отказ контрольно-измерительных приборов, автоматики безопасности, сигнализации и блокировок на газоиспользующих установках; - остановка технологических агрегатов и производственных процессов вследствие отказа в работе оборудования, механизмов, средств автоматики регулирования и контроля; - отказ или повреждение деталей и узлов технических устройств, - утечка технологических газов, продуктов разделения воздуха, получаемых или используемых в технологическом процессе, по причине нарушения герметичности трубопроводов, технических устройств Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	6 Внезапное обрушение зданий и сооружений 6.1 Внезапное обрушение производственных зданий и сооружений 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
	ОПО тепло-, электроэнергетики Состояние технологических систем (цех №, установка №): - сообщение об аварии/инциденте (устранении инцидента) в технологической системе — параметр(ы) процесса, вышедший(ие)/вернувшийся(еся) за аварийные/предупредительные уставки: параметры расхода, температуры, давления и температуры в установках, уровни в емкостях пожароопасных и вредных веществ, уровни в дренажных стоках и канализационных колодцах, параметры электроснабжения, тепло-, водо- и газоснабжения оборудования, давления воздуха контрольно-измерительных приборов и аппаратуры; - нарушения требований нормативных правовых актов Российской Федерации, а также нормативных технических документов, устанавливающих правила ведения работ ОПО:	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 6 Внезапное обрушение зданий, сооружений, пород 6.1 Обрушение элементов транспортных коммуникаций 6.2 Обрушение производственных зданий и сооружений 8 Аварии на электроэнергетических системах 8.1 Аварии на автономных электростанциях с долговременным перерывом электроснабжения потребителей

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	параметры пожаро- и газоопасности, параметры концентрации вредных веществ в производственных помещениях и рабочей зоне установок; - отказ или повреждение деталей и узлов технических устройств; - отказ (выход из строя) газового оборудования (технических устройств) газорегуляторных пунктов и установок; - повреждения технических устройств (взрывных клапанов) при розжиге газоиспользующих установок (котлов, печей, агрегатов); - повреждения крышек и затворов у лазов или люков паровых котлов и сосудов, работающих под давлением; топочных камер, жаровых труб котлов, сосудов, работающих под давлением; - отказ контрольно-измерительных приборов, автоматики безопасности, сигнализации и блокировок на газоиспользующих установках Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	8.2 Аварии на электроэнергетических системах (сетях) с долговременным перерывом электроснабжения основных потребителей и обширных территорий 8.3 Выход из строя транспортных электрических контактных сетей 9 Аварии на коммунальных системах жизнеобеспечения 9.2 Аварии в системах снабжения населения питьевой водой 9.3 Аварии на тепловых сетях (системах горячего водоснабжения) в холодное время года 9.4 Аварии на коммунальных газопроводах 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
	ОПО добычи полезных ископаемых Состояние технологических систем (цех №, установка №): - сообщение об аварии/инциденте (устранении инцидента) в технологической системе — параметр(ы) процесса, вышедший(ие)/вернувшийся(еся) за аварийные/предупредительные уставки: параметры конвейерного транспорта (скорости, натяжения лент, боковой сход ленты, ограждения, датчики экстренного останова), уровень транспортируемого материала в местах перегрузок, параметры вибрации, сдвига, зазоров, частоты вращения оборудования (насосные станции),	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.4 Пожары (взрывы) в шахтах, подземных выработках, метрополитенах 2 Аварии с выбросом (угрозой выброса) опасных веществ 2.5 Внезапные выбросы метана, углекислого газа и других ядовитых веществ и газов 6 Внезапное обрушение зданий, сооружений, пород 6.1 Обрушение элементов транспортных коммуникаций

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов. Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	параметры концентраций, температуры, расхода и давления в установке, параметры газоиспользующего оборудования (погасание факела горелок, давление газа перед горелкой), уровни в емкостях пожароопасных и вредных веществ, уровни в зумпфах, дренажных емкостях, приямках и канализационных колодцах, параметры электроснабжения, тепло-, водо- и газоснабжения оборудования, давления воздуха контрольно-измерительных приборов и аппаратуры; - нарушения требований нормативных правовых актов Российской Федерации, а также нормативных технических документов, устанавливающих правила ведения работ на ОПО: параметры пожаро- и газоопасности; параметры концентрации вредных веществ в производственных помещениях и рабочей зоне установок; - обрыв и короткое замыкание в цепях управления оборудованием; - параметры газоиспользующего оборудования (погасание факела горелок, давление газа перед горелкой) Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	6.2 Обрушение производственных зданий и сооружений 6.3 Обрушение пород и полезных ископаемых в горных выработках, включая карьеры 6.4 Авария на подземном сооружении 11 Гидродинамические аварии 11.3 Прорывы плывунов, пульпы и глинистой массы, а также затопление водой действующих горных выработок при разработке полезных ископаемых 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
	ГТС Состояние условий эксплуатации ГТС [сообщение об аварии/инциденте (устранении инцидента)]: - показатели нарушений нормальной эксплуатации ГТС с установленной периодичностью контроля: параметры контроля состояния ГТС и прилегающей территории (количественные и качественные показатели состояния ГТС), вышедшие/вернувшиеся за предупредительные/аварийные уставки, соответствующие критериям безопасности I/II уровня, заданным в декларации безопасности ГТС),	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 6 Внезапное обрушение зданий, сооружений, пород 6.1 Обрушение элементов транспортных коммуникаций

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	характеристики состояния технических средств (положения и перекосы механизмов, токи в двигателях механизмов, температура и давление рабочей жидкости в насосных и моторных агрегатах гидроприводов), нарушения в автоматизированной системе контроля и управления АСУ ТП (судопропуска — для судоходных ГТС), параметры электроснабжения оборудования и цепей управления, давления воздуха контрольно-измерительных приборов и аппаратуры, уровни в емкостях пожароопасных и вредных продуктов (баки маслонапорных установок гидроприводов затворов); - повреждение ГТС, приведшее к нарушению его безопасной эксплуатации и вызвавшее понижение уровня воды в водохранилище (реке) или повышение его в нижнем бьефе за предельно допустимые значения Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	6.2 Обрушение производственных зданий и сооружений 7 Транспортные аварии (катастрофы) Примечание — Для судоходных ГТС 11 Гидродинамические аварии 11.1 Прорывы плотин (дамб, шлюзов, перемычек и др.) с образованием волн прорыва и катастрофических затоплений 11.2 Прорывы плотин (дамб, шлюзов, перемычек и др.) с образованием прорывного паводка 11.3 Прорывы плывунов, пульпы и глинистой массы, а также затопление водой действующих горных выработок при разработке полезных ископаемых 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
	ОИАЭ Обобщенный сигнал «Авария в технологических процессах»: - тип и характеристики аварии (по факту): воздействие стихийных бедствий, которое может повлечь радиационную аварию, пожар, который может повлечь радиационную аварию, возможные террористические действия, которые могут повлечь радиационную аварию; - объявление состояний «Аварийная готовность», «Аварийная обстановка» Состояние системы, обеспечивающей технологические процессы:	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 4 Аварии с выбросом (угрозой выброса) РВ 4.1 Аварии на атомных электростанциях, промышленных и исследовательских ядерных установках с выбросом (угрозой выброса) РВ 4.2 Аварии с выбросом (угрозой выброса) РВ на предприятиях ядерно-топливного цикла

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов. Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	- сообщение об аварии/происшествии определенной категории (А04/П01) (устранении аварии/происшествия) в технологической системе — параметр(ы) процесса, вышедший(ие)/вернувшийся(еся) за предупредительные/аварийные уставки по критериям происшествия/аварии определенной категории; - нарушение нормальных условий эксплуатации [запуск технологических систем безопасности, отказы систем (элементов)]; - информация объектовой АСУ ТП верхнего уровня о состоянии технологического оборудования и систем Радиационное состояние ОИАЭ: - сообщение о происшествии по критериям происшествия определенной категории (П01); - сообщение об аварии по критериям аварии определенной категории (А04); - сообщение об объявлении состояния «Аварийная готовность»; - сообщение об объявлении состояния «Аварийная обстановка» Примечание — Критерии происшествий, аварий и объявления состояний «Аварийная готовность» и «Аварийная обстановка» устанавливаются в соответствии с федеральными нормами и правилами в области использования атомной энергии, определяющими порядок объявления аварийной обстановки Состояние АСУ ТП: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	4.3 Аварии транспортных средств и космических аппаратов с ядерными установками или грузом РВ на борту 4.4 Аварии на пунктах хранения ядерных материалов и РВ, хранилищах отработавшего ядерного топлива, пунктах хранения или захоронения радиоактивных отходов 4.5 Обнаружение (утрата) источников ионизирующих излучений 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе системах связи, противопожарной защиты и безопасности 12.1 Аварии в технологических системах 12.2 Аварии в системах инженерно-технического обеспечения
Системы инженерно-технического обеспечения объекта 1 Система электроснабжения 1.1 Система общего электроснабжения; 1.2 Система бесперебойного электроснабжения 1.3 Система гарантированного электроснабжения	Состояние систем инженерно-технического обеспечения: - сигнал/снятие сигнала о нарушении работоспособности основного оборудования (установок) — параметры основного оборудования (электротехнические, термодинамические, вибродиагностические, аэрозольные), вышедшие/вернувшиеся за аварийные/предупредительные уставки;	

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
2 Система электроосвещения 2.1 Система внутреннего электроосвещения 2.2 Система внешнего электроосвещения 3 Система теплоснабжения объекта 4 Система холодоснабжения 5 Система отопления, вентиляции, кондиционирования, тепловых сетей 6 Система водоснабжения 7 Система водоотведения 8 Система вертикального транспорта 9 Система газоснабжения 10 Автоматизированная система диспетчеризации и управления объектом Сигналы ПК СМИС: - сигнал «Авария/инцидент» в системах инженерно-технического обеспечения; - обобщенный сигнал «Авария» в системах инженерно-технического обеспечения Примечания 1 Сигнал «Авария/инцидент» формируется в автоматизированном режиме ПК СМИС 2 Обобщенный сигнал «Авария» формируется по факту оперативным персоналом СМИС Код состояния (статуса) события: 100 — инцидент; 110 — авария; 200 — снятие с регистрации; 111 — обобщенный сигнал «Авария», формируемый оперативным персоналом по факту аварии	- регламентированное время восстановления работоспособности (параметров) оборудования (процесса) Состояние автоматизированной системы диспетчеризации и управления объектом: - нарушение/восстановление работоспособности системы (отсутствие/восстановление электроснабжения шкафов, контроллеров, серверов)	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов 1.5 Пожары (взрывы) в зданиях и сооружениях жилого, социально-бытового, культурного назначения 8 Аварии на электроэнергетических системах 9 Аварии на коммунальных системах жизнеобеспечения 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.2 Аварии в системах инженерно-технического обеспечения
Системы противопожарной защиты 1 Автоматизированный комплекс управления системами противопожарной защиты 2 Система пожарной сигнализации	Состояние систем противопожарной защиты: - сообщение об аварии/ликвидации аварии в системах противопожарной защиты в пожарной зоне А: нарушение/восстановление работоспособности основных технических устройств и (или) каналов (линий) связи,	Z = 1; K = 1; V = 1 Пожары и взрывы (с возможным последующим горением) 1.1 Пожары (взрывы) в зданиях, на коммуникациях и в технологическом оборудовании промышленных объектов

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов. Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
3 Система оповещения и управления эвакуацией 4 Система противопожарного водоснабжения 5 Система автоматического пожаротушения 5.1 Система автоматического водяного пожаротушения 5.2 Система газового пожаротушения 5.3 Система порошкового пожаротушения 6 Система противодымной защиты объекта Сигналы ПК СМИС: - сигнал «Авария/инцидент», - сигнал «Пожар», - обобщенный сигнал «Авария» Код состояния (статуса) события: 100 — инцидент, 110 — авария, 130 — пожар; 200 — снятие с регистрации, 131 — обобщенный сигнал «Пожар»	отсутствие/восстановление электроснабжения насосов (рабочих, резервных, жокей-насосов), отсутствие питания в цепях управления насосами, задвижками, клапанами, сигнал «Утечка из системы», отсутствие питания в цепях управления вентиляторами, клапанами; - сигнал «Пожар»; - обобщенный сигнал «Авария в системах противопожарной защиты» (отказ системы); - несрабатывание системы противопожарного водоснабжения при получении сигнала «Пожар» от пожарной сигнализации (с указанием места); - несрабатывание насосов автоматического водяного пожаротушения при срабатывании реле давления; - несрабатывание систем автоматического газового, порошкового пожаротушения, противопожарной вентиляции при получении сигнала «Пожар» (с указанием места); - регламентированное время восстановления работоспособности системы (оборудования) систем противопожарной защиты (пожарной сигнализации, оповещения и управления эвакуацией, противопожарного водоснабжения; автоматического пожаротушения; противопожарной вентиляции)	1.5 Пожары (взрывы) в зданиях и сооружениях жилого, социально-бытового, культурного назначения 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.3 Аварии в системе противопожарной защиты
Системы связи и оповещения объекта 1 Система диспетчерской (технологической, производственной громкоговорящей) связи 2 Система транкинговой радиосвязи 3 Система оповещения и поиска персонала 4 Система радиотрансляции Сигналы ПК СМИС: - обобщенный сигнал «Авария» формируется по факту оперативным персоналом СМИС;	Состояние систем и сетей связи — сообщение об аварии/инциденте в системах связи объекта: - отказ в соединительной линии системы диспетчерской (технологической, громкоговорящей) связи; - блокировка/разблокировка неисправных соединительных линий, ведущих к автоматической телефонной станции (коммутатору); - отказ оборудования блоков автоматической телефонной станции; - обобщенный сигнал о неработоспособности всех базовых станций и всех коммутационных станций системы транкинговой радиосвязи;	Z = 1; K = 1; V = 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.4 Аварии в системах связи и оповещения

Продолжение таблицы К.1

Объект контроля угроз возникновения аварий и ЧС Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
- сигнал «Инцидент» формируется в автоматизированном режиме ПК СМИС	- обобщенный сигнал о неработоспособном состоянии системы оповещения и поиска персонала, системы радиотрансляции; - нарушение работоспособности системы/отсутствие оповещения персонала и населения об угрозе ЧС	
Системы безопасности (физической защиты) объекта 1 Система управления доступом и охранной сигнализации 2 Система охранного телевидения 3 Система обнаружения химического, радиоактивного заражения объекта Сигналы ПК СМИС: - сигнал «Инцидент»; - обобщенный сигнал «Авария»; - сигнал от кнопки «Тревога»	Состояние систем безопасности (физической защиты): - сообщение об инциденте/ликвидации инцидента в системе — отказы и/или повреждения деталей и узлов технических устройств (оборудования); - обобщенный сигнал/снятие сигнала о неработоспособном состоянии системы; - террористические проявления; - обнаружение химического, радиоактивного заражения объекта	Z = 1; K = 1; V = 12 Аварии в технологических системах и системах инженерно-технического обеспечения, в том числе в системах связи, противопожарной защиты и безопасности 12.5 Аварии в системах безопасности (физической защиты) Z = 3; K = 3; V = 1 Террористические проявления 1.1 Без определения — сигнал от кнопки «Тревога» 1.2 Несанкционированное проникновение на объект 1.4 Угроза газовой атаки 1.18 Обнаружение источников ионизирующего излучения
Строительные (несущие) конструкции и основания зданий и сооружений объекта Сигналы ПК СМИС: - сигнал «Авария/инцидент», - обобщенный сигнал «Авария»	Состояние строительных (несущих) конструкций и оснований зданий и сооружений: - предаварийное состояние строительных (несущих) конструкций и оснований зданий и сооружений объекта — параметры контроля состояния (показатели нарушений нормальной эксплуатации с установленной периодичностью контроля), вышедшие за предупредительные уставки; - аварийное состояние строительных (несущих) конструкций и оснований зданий и сооружений объекта — параметры контроля состояния (показатели	Z = 1; K = 1; V = 6.1 Обрушение элементов транспортных коммуникаций 6.2 Обрушение производственных зданий и сооружений 6.3 Обрушение зданий и сооружений жилого, социально-бытового и культурного назначения 12.6 Авария в системе мониторинга строительных (несущих) конструкций и оснований зданий и сооружений объекта

Окончание таблицы К.1

Объект контроля угроз возникновения аварий и ЧС. Сигналы ПК СМИС Код состояния (статуса) события	Тип и ведомственная принадлежность объектов. Контролируемые факторы (параметры)	Угроза перерастания аварии в ЧС (Z, K, V) по классификатору угроз СМИС Код события
	нарушений нормальной эксплуатации с установленной периодичностью контроля), вышедшие за аварийные уставки Изменение работоспособности системы мониторинга строительных (несущих) конструкций и оснований зданий и сооружений объекта: - сообщение об аварии/инциденте (ликвидации инцидента) в системе; - отказы и/или повреждения деталей и узлов технических устройств (оборудования); - обобщенный сигнал/снятие сигнала о неработоспособном состоянии системы	

Библиография

[1] Протокол SOAP (простой протокол доступа к объектам). [Электронный ресурс] // Simple Object Access Protocol (SOAP) 1.1. URL: (дата обращения: 14 ноября 2018 г.)

[2] Безопасность веб-сервисов. Web Services Security: SOAP Message Security 1.0 [Электронный ресурс] // (WS-Security 2004) OASIS Standard 200401. URL: gost.e-ecolog.ru gost.e-ecolog.ru ата обращения: 14 ноября 2018 г.)

[3] WSDL (язык описания web-сервисов и доступа к ним, основанный на языке XML). [Электронный ресурс] // Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. W3C Recommendation 26 June 2007. URL: gost.e-ecolog.ru (дата обращения: 14 ноября 2018 г.)

[4] Безопасность веб-сервисов. Web Services Security: X.509 Certificate Token Profile 1.1 OASIS Standard Specification [Электронный ресурс] // URL: gost.e-ecolog.ru ; Web Services Security X.509 Certificate Token Profile OASIS Standard 200401 [Электронный ресурс] // URL: gost.e-ecolog.ru oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf (дата обращения: 14 ноября 2018 г.)

[5] Стандарт для инфраструктуры открытого ключа и инфраструктуры управления привилегиями. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [Электронный ресурс] // URL: http:// gost.e-ecolog.ru (дата обращения: 14 ноября 2018 г.)

[6] Постановление Правительства РФ «О классификации чрезвычайных ситуаций природного и техногенного характера» от 21 мая 2007 г. № 304

[7] Постановление Правительства РФ «О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 24 марта 1997 г. № 334 (с изменениями и дополнениями)

[8] Приказ МЧС России «Об утверждении критериев информации о чрезвычайных ситуациях» от 8 июля 2004 г. № 329

[9] Приказ МЧС России «Об утверждении Требований по предупреждению чрезвычайных ситуаций на потенциально опасных объектах и объектах жизнеобеспечения» от 28 февраля 2003 г. № 105

УДК 658.382.3.006.354 ОКС 13.200

Ключевые слова: система мониторинга инженерных систем зданий и сооружений, органы повседневного управления РСЧС, программные комплексы, технические требования, протоколы информационного обмена, веб-сервис, классы сообщений, классификатор событий

БЗ 3—2019/26

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 19.11.2019. Подписано в печать 15.01.2020 Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,02
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru