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

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 22.1.15— 2025

Безопасность в чрезвычайных ситуациях

ТЕХНИЧЕСКИЕ СРЕДСТВА МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ПРИРОДНОГО И ТЕХНОГЕННОГО ХАРАКТЕРА

Классификация. Общие технические требования

Издание официальное

Москва
Российский институт стандартизации
2026

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России» (Федеральный центр науки и высоких технологий) [ФГБУ ВНИИ ГОЧС (ФЦ)]

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 071 «Гражданская оборона, предупреждение и ликвидация чрезвычайных ситуаций»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 29 декабря 2025 г. № 192-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узбекское агентство по техническому регулированию

4 Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2025 г. № 1861-ст межгосударственный стандарт ГОСТ 22.1.15—2025 введен в действие в качестве национального стандарта Российской Федерации с 1 апреля 2026 г.

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

© Оформление. ФГБУ «Институт стандартизации», 2026

В Российской Федерации 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

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

Безопасность в чрезвычайных ситуациях

ТЕХНИЧЕСКИЕ СРЕДСТВА МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ПРИРОДНОГО И ТЕХНОГЕННОГО ХАРАКТЕРА

Классификация.
Общие технические требования

Safety in emergencies. Technical tools of natural and technological emergencies monitoring. Classification. General technical requirements

Дата введения — 2026—04—01

1 Область применения

1.1 Настоящий стандарт распространяется на технические средства мониторинга чрезвычайных ситуаций (ЧС) природного и техногенного характера.

1.2 Настоящий стандарт устанавливает классификацию и общие технические требования к техническим средствам мониторинга ЧС природного и техногенного характера (ТСМ ЧС).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие межгосударственные стандарты:

ГОСТ 2.601 Единая система конструкторской документации. Эксплуатационные документы

ГОСТ 14192 Маркировка грузов

ГОСТ 14254 (IEC 60529:2013) Степени защиты, обеспечиваемые оболочками (Код IP)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации (gost.e-ecolog.ru ю указателям национальных стандартов, издаваемым в государствах, указанных в предисловии, или на официальных сайтах соответствующих национальных органов по стандартизации. Если на документ дана недатированная ссылка, то следует использовать документ, действующий на текущий момент, с учетом всех внесенных в него изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то следует использовать указанную версию этого документа. Если после принятия настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение применяется без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **технические средства мониторинга чрезвычайных ситуаций;** ТСМ ЧС: Изделия, устройства, приборы и информационно-вычислительные (программно-технические) комплексы, предназначенные для обеспечения наблюдения за окружающей средой, техногенными объектами с целью оценки, анализа и своевременного выявления изменений их состояния, происходящих в них процессов

Издание официальное

и явлений, а также для информационной поддержки при принятии решений по предупреждению и ликвидации чрезвычайных ситуаций.

3.1.2 **датчики и измерительные средства контроля изменения состояния параметров окружающей среды или отдельных ее компонентов;** ДИС: Изделия, приборы, инструменты и аппараты, осуществляющие контроль параметров, характеризующих потенциальную опасность источников чрезвычайных ситуаций.

3.1.3 **средства передачи данных;** СПД: Устройства и аппаратура, обеспечивающая доведение сообщений об опасном изменении параметров окружающей среды или отдельных ее компонентов, характеризующих потенциальную опасность источников чрезвычайных ситуаций, через органы управления по чрезвычайным ситуациям объектов эксплуатации до органов управления по чрезвычайным ситуациям государственной власти.

3.1.4 **информационно-вычислительные (программно-технические) комплексы мониторинга;** ИВК: Вычислительные машины и их блоки, осуществляющие информационную поддержку принятия решений на уровне органов управления по чрезвычайным ситуациям государственной власти, органов управления по чрезвычайным ситуациям объектов эксплуатации, по недопущению чрезвычайных ситуаций и ликвидации их последствий.

3.1.5 **орган управления по чрезвычайным ситуациям;** ОУЧС: Орган, предназначенный для выполнения задач по управлению мероприятиями по защите от чрезвычайных ситуаций природного и техногенного характера.

3.1.6 **объект эксплуатации:** Объект капитального строительства, линейный объект, на котором эксплуатируются технические средства мониторинга чрезвычайных ситуаций.

3.1.7 **техногенный объект:** Объект, созданный человеком в процессе производственно-хозяйственной деятельности, и способный оказывать негативное воздействие на окружающую среду.

3.2 В настоящем стандарте применены следующие сокращения:

Ethernet — семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей (см. [1])

HTTP — сетевой протокол прикладного уровня сетевой модели OSI (см. [2])

IPv4 — четвертая версия интернет-протокола (см. [3])

LAN — локальная вычислительная сеть (см. [1])

OSI — базовая эталонная модель взаимосвязи открытых систем (см. [4])

SOAP — протокол обмена сообщениями в формате XML (см. [5])

RS-232 — стандарт физического уровня сетевой модели OSI передачи данных (см. [6])

RS-485 — стандарт физического уровня сетевой модели OSI передачи данных (см. [7])

TCP — транспортный протокол, который обеспечивает надежную и упорядоченную передачу данных по сети (см. [8])

X.509 — стандартизированный формат цифровых сертификатов, которые используются для обеспечения безопасности при передаче данных (см. [9], [10])

WS-Security — спецификация безопасности для протокола SOAP (см. [11])

4 Классификация

4.1 ТСМ ЧС подразделяют:

а) по функциональному назначению;

б) условиям эксплуатации.

4.2 По функциональному назначению ТСМ ЧС подразделяют:

а) на датчики и измерительные средства контроля изменения состояния параметров окружающей среды или отдельных ее компонентов;

б) средства передачи данных;

в) информационно-вычислительные (программно-технические) комплексы мониторинга.

4.3 По условиям эксплуатации ТСМ ЧС подразделяют:

а) на эксплуатируемые в телекоммуникационных шкафах (помещениях, сооружениях) с регулируемым микроклиматом;

б) эксплуатируемые в телекоммуникационных шкафах (помещениях, сооружениях) с нерегулируемым микроклиматом;

в) эксплуатируемые на открытых пространствах.

5 Общие технические требования

5.1 Основные показатели и/или характеристики (свойства)

5.1.1 Показатели назначения

5.1.1.1 Критерием функциональности ДИС должно являться обеспечение выдачи выходного сигнала на ИВК ОУЧС объектов эксплуатации.

5.1.1.2 Критерием функциональности СПД должно являться обеспечение передачи данных между ИВК ОУЧС объектов эксплуатации и ИВК ОУЧС государственной власти.

5.1.1.3 Критериями функциональности ИВК ОУЧС объектов эксплуатации должны являться:

а) прием выходного сигнала ДИС;

б) обмен SOAP сообщениями с ИВК ОУЧС государственной власти;

в) обеспечение визуализации информационных материалов поддержки принятия решений на уровне ОУЧС объектов эксплуатации.

5.1.1.4 Критериями функциональности ИВК ОУЧС государственной власти должны являться:

а) обмен SOAP сообщениями с ИВК ОУЧС объектов эксплуатации;

б) обеспечение визуализации информационных материалов поддержки принятия решений на уровне ОУЧС государственной власти.

5.1.1.5 Для совместимости и информационно-технического сопряжения ДИС с ИВК ОУЧС объектов эксплуатации ДИС должны обеспечивать выдачу выходного сигнала в одном из следующих форматах: 4-20 мА, 0-5 В, 0-10 В, DI, FDI, RS-232, RS-485.

5.1.1.6 Для совместимости и информационно-технического сопряжения СПД с ИВК ОУЧС объектов эксплуатации, ИВК ОУЧС государственной власти СПД должны обеспечивать:

а) передачу данных в сетях не ниже LAN с архитектурой сетевой модели OSI;

б) на канальном уровне взаимодействия сетевой модели OSI работу протокола не ниже Ethernet;

в) на сетевом уровне взаимодействия сетевой модели OSI работу протокола не ниже IPv4;

г) на транспортном уровне взаимодействия сетевой модели OSI работу протокола TCP.

5.1.1.7 Для совместимости и информационно-технического сопряжения ИВК ОУЧС объектов эксплуатации с ИВК ОУЧС государственной власти ИВК должны обеспечивать на прикладном уровне взаимодействия сетевой модели OSI обмен SOAP сообщениями по протоколу HTTP.

5.1.1.8 В состав программного обеспечения ИВК ОУЧС государственной власти должен входить веб-сервер, обеспечивающий работу веб-сервиса для обмена SOAP сообщениями между ИВК. Описание веб-сервиса приведено в приложении А.

5.1.1.9 Для управления рисками и прогнозирования ЧС, оценки эффективности предупреждения ЧС по результатам мониторинга в программном обеспечении ИВК должны быть предусмотрены средства, позволяющие просматривать информационные материалы поддержки принятия решений в следующих файловых форматах: *.pdf, *.odt, *.rtf, *.doc, *.docx, *.txt, *.tiff, *.jpg, *.png, *.obj, *.fbx, *.stl, *.amf, *.iges, *.dwf, *.dwfx, *.vsdx, *.mp4, *.mov, *.avi, *.mkv.

5.1.1.10 Для защиты информации от несанкционированного доступа СПД должны обладать способностью, обеспечивающей идентификацию и аутентификацию пользователя с использованием логина и пароля для доступа к управлению их настройками.

5.1.1.11 Для защиты информации от несанкционированного доступа в программном обеспечении ИВК должны быть предусмотрены средства, обеспечивающие:

а) идентификацию и аутентификацию пользователей с использованием логинов и паролей для доступа к ИВК;

б) антивирусную проверку, обновление антивирусной базы с использованием доступа к сети Интернет.

5.1.1.12 Для защиты конфиденциальности и целостности информации в программном обеспечении ИВК должны быть предусмотрены средства, обеспечивающие шифрование и электронно-цифровую подпись передаваемых SOAP сообщений.

5.1.1.13 Шифрование и электронно-цифровая подпись SOAP сообщений должны быть реализованы посредством обмена ИВК сертификатами безопасности X.509 и использования спецификации WS-Security.

5.1.1.14 В случае возникновения ошибки передачи данных в программном обеспечении ИВК должны быть предусмотрены алгоритмы, обеспечивающие:

а) сохранение передаваемой информации в очереди (базах данных);

б) цикличный повтор попыток передачи информации из очереди вплоть до успешного завершения данной операции;

в) очистку очереди при успешной передаче всей информации.

5.1.1.15 Средняя задержка выходного сигнала ДИС не должна превышать 30 с.

5.1.1.16 В ТСМ ЧС соответственно должно быть предусмотрено:

а) в ИВК ОУЧС объектов эксплуатации диагностирование состояния подключенных ТСМ ЧС;

б) в ИВК ОУЧС органов государственной власти диагностирование состояния подключенных ТСМ ЧС;

в) в ИВК ОУЧС объектов эксплуатации диагностирование состояния сторонних подключений;

г) в ИВК ОУЧС объектов эксплуатации диагностирование состояния готовности его пользователя к выполнению своих функциональных обязанностей.

5.1.1.17 Все выполняемые ИВК функции, задачи (комплексы задач), процедуры должны иметь экранные формы в интерфейсе программного обеспечения ИВК.

5.1.2 Конструктивные требования

5.1.2.1 В конструкции ТСМ ЧС должны отсутствовать острые выступающие части, углы, кромки и поверхности с неровностями, которые могут нанести повреждения персоналу.

5.1.3 Требования к надежности

5.1.3.1 Среднее время наработки на отказ ТСМ ЧС должно составлять не менее 10 000 ч.

5.1.3.2 Коэффициент готовности ТСМ ЧС должен составлять не менее 99,8 %.

5.1.4 Требования к стойкости к внешним воздействиям и живучести

5.1.4.1 ТСМ ЧС должны выдерживать, не теряя своих технических характеристик, синусоидальную вибрацию частотой от 1 до 70 Гц.

5.1.4.2 ТСМ ЧС, эксплуатируемые в телекоммуникационных шкафах (помещениях, сооружениях) с регулируемым микроклиматом, должны иметь степень защиты не ниже IP30 по ГОСТ 14254 и сохранять функциональность:

а) при температуре окружающей среды от плюс 5 °С до плюс 35 °С;

б) относительной влажности воздуха от 45 % до 75 %.

5.1.4.3 ТСМ ЧС, эксплуатируемые в телекоммуникационных шкафах (помещениях, сооружениях) с нерегулируемым микроклиматом, должны иметь степень защиты не ниже IP50 по ГОСТ 14254 и сохранять функциональность:

а) при температуре окружающей среды от минус 50 °С до плюс 50 °С;

б) относительной влажности воздуха от 45 % до 75 %.

5.1.4.4 ТСМ ЧС, эксплуатируемые на открытых пространствах, должны иметь степень защиты не ниже IP65 по ГОСТ 14254 и сохранять функциональность:

а) при температуре окружающей среды от минус 50 °С до плюс 50 °С;

б) относительной влажности воздуха от 30 % до 95 %.

5.1.4.5 ТСМ ЧС должны сохранять функциональность при электроснабжении от источников бесперебойного питания в течение не менее 2 ч.

5.1.4.6 ТСМ ЧС должны сохранять функциональность при допустимых отклонениях напряжения сети электроснабжения от минус 15 % до плюс 10 %.

5.2 Комплектность

5.2.1 В комплект поставки должны входить:

- ТСМ ЧС в собранном виде;
- эксплуатационные документы в соответствии с требованиями ГОСТ 2.601.

5.2.2 ДИС, СПД должны комплектоваться эксплуатационной документацией в следующем составе:

а) руководство по эксплуатации;

б) инструкция по монтажу, пуску, регулированию и обкатке;

в) паспорт;

г) нормы расхода запасных частей;

д) нормы расхода материалов;

ж) ведомость комплекта запасных частей, инструментов и принадлежностей;

и) инструкции эксплуатационные специальные;

к) ведомость эксплуатационных документов.

5.2.3 ИВК должны комплектоваться эксплуатационной документацией в следующем составе:

а) инструкция по эксплуатации комплекса;

б) формуляр;

в) паспорт;

г) ведомость эксплуатационных документов.

5.2.4 Программное обеспечение ИВК должно комплектоваться эксплуатационной документацией в следующем составе:

а) формуляр;

б) описание применения;

в) руководство системного программиста;

г) руководство программиста;

д) руководство пользователя (оператора);

е) ведомость эксплуатационных документов.

5.2.5 В эксплуатационной документации на ТСМ ЧС должна содержаться следующая информация:

а) коэффициент готовности;

б) назначенный срок службы.

5.2.6 Комплект поставки ТСМ ЧС должен обеспечивать их монтаж без применения нестандартного оборудования и нестандартных инструментов. В случае необходимости применения нестандартных инструментов они должны входить в комплект поставки.

5.3 Маркировка

5.3.1 На ТСМ ЧС должна быть нанесена маркировка, содержащая следующую информацию:

а) наименование продукции и ее тип (вид), марка, модель;

б) наименование страны-изготовителя;

в) дату изготовления продукции (месяц, год).

5.3.2 На упаковку ТСМ ЧС должна быть нанесена маркировка, содержащая следующую информацию:

а) местонахождение и адрес юридического лица, являющегося изготовителем [адрес места осуществления деятельности (в случае, если адреса различаются), номера телефона и (или) адреса электронной почты];

б) номер партии продукции;

в) срок службы;

г) товарный знак (при наличии).

5.3.3 Маркировка должна быть нанесена на русском языке и при наличии соответствующих требований в законодательстве государств — членов ЕАСС на государственном языке (государственных языках) государства — члена ЕАСС, на территории которого выпускается в обращение продукция.

5.3.4 Маркировка продукции должна быть разборчивой, легкочитаемой и нанесена в доступном для осмотра месте.

5.3.5 Для ТСМ ЧС, эксплуатируемых на открытых пространствах, маркировка должна сохраняться в течение назначенного срока службы.

5.4 Упаковка

5.4.1 ТСМ ЧС должно быть упаковано в тару. Упаковка не должна иметь острых выступающих частей, углов, кромок и поверхностей с неровностями, которые могут нанести повреждения транспортным средствам, их внутреннему оборудованию, упаковке других грузовых мест и обслуживающему персоналу.

5.4.2 Маркировку тары выполняют по ГОСТ 14192.

Приложение А
(обязательное)

Описание веб-сервиса ИВК ОУЧС государственной власти

Структура веб-сервиса должна иметь вид:

```
<?xml version="1.0" encoding="WINDOWS-1251"?>
<wsdl:definitions xmlns:xsd="gost.e-ecolog.ru "
xmlns:wsdl="gost.e-ecolog.ru "
xmlns:tns="gost.e-ecolog.ru "
xmlns:soap="gost.e-ecolog.ru "
xmlns:ns1="gost.e-ecolog.ru "
targetNamespace="gost.e-ecolog.ru "
name="DispatchServiceImplService">
<wsdl:types>
<xs:schema xmlns:tns="gost.e-ecolog.ru "
targetNamespace="gost.e-ecolog.ru "
xmlns:xs="gost.e-ecolog.ru " 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:DispatchControlPointReqiiest">
</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>
```

Библиография

[1]	ISO/IEC/IEEE 8802-3:2021	Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks — Part 3: Standard for Ethernet
[2]	IETF RFC 2616 June 1999	IETF Hypertext Transfer Protocol — HTTP/1.1
[3]	IETF RFC 791	(IP) «Internet Protocol», J. Postel, 01.09.1981
[4]	ISO/IEC 7498-1:1994	Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model
[5]	IETF RFC 4227 January 2006	Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)
[6]	EIA/TIA-232-F	Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange/Note: Approved 2002-10-11
[7]	ANSI TIA/EIA-485-A:1998	Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems
[8]	IETF RFC 793 September 1981	Transmission control protocol darpa internet program protocol specification (TCP), J. Postel
[9]	IETF/RFC 3280 April 2002	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[10]	IETF RFC 5280 May 2008	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[11]	OASIS Standard 200401 March 2004	Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)

УДК 614.8:006.354 МКС 13.200

Ключевые слова: мониторинг чрезвычайных ситуаций, предупреждение чрезвычайных ситуаций, технические средства мониторинга чрезвычайных ситуаций, классификация, технические требования

Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 12.01.2026. Подписано в печать 09.02.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,50.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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