Internet Engineering Task Force (IETF)
Request for Comments: 8632
Category: Standards Track
ISSN: 2070-1721

S. Vallin
Stefan Vallin AB
M. Bjorklund
Cisco

September 2019

A YANG Data Model for Alarm Management

Модель данных YANG для сигналов тревоги

Аннотация

Этот документ задаёт модуль YANG для управления сигналами тревоги. Модуль включает функции для управления списком сигналов, блокировки аварийных сигналов и уведомления систем управления. Имеются также операции для управления состоянием оператора сигналов тревоги и процедуры административных аварийных сигналов. Модуль сопоставляется с соответствующими стандартами для аварийных сигналов.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8632.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Этот документ задаёт модуль YANG [RFC7950] для управления сигналами тревоги. Цель состоит в определении стандартизованного интерфейса для аварийных сигналов в сетевых устройствах, который можно легко интегрировать с управляющими приложениями. Модель также применима для северного интерфейса в управляющих приложениях.

Отслеживание аварийных сигналов является важной частью мониторинга сети. Необработанные сигналы от устройств не всегда указывают состояние сетевых служб и первопричину. Возможность передачи сигналов в приложения управления аварийными сигналами в стандартизованном формате является отправной точкой для выполнения высокоуровневых задач обеспечения надёжности сети.

Устройство модуля основано на опыте реализации и применения доступных аварийных сигналов из стандартов ITU [X.733], 3GPP [ALARMIRP] и ANSI [ISA182].

1.1. Термины и обозначения

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

Ниже перечислены термины, определённые в [RFC7950]:

- action - действие;
- client - клиент;
- data tree - дерево данных;
- server - сервер.

Этот документ определяет ряд дополнительных терминов.

Alarm (общая концепция) - сигнал тревоги, аварийный сигнал
Указывает нежелательное состояние ресурса, требующее корректировки.

Fault - отказ
Причина нежелательного поведения. Не существует нетривиальной взаимно-однозначной связи между аварийными сигналами и отказами. Один отказ может вызывать несколько сигналов тревоги, если в системе нет возможности определить первопричину и найти корреляции. Для аварийного сигнала может не быть отказа, послужившего причиной. Например, сигнал о неприемлемой средней оценке (Mean Opinion Score или MOS) от зонда Voice over IP (VOIP) в результате неоптимальной настройки качества обслуживания (QoS).

Alarm Type - тип сигнала тревоги
Тип сигнала указывает возможное уникальное состояние тревоги для ресурса. Типы сигналов указываются именами, такими как link-alarm (тревога на канале), jitter-violation (нарушение допустимых вариаций), high-disk-utilization (значительное заполнение диска).

Resource - ресурс
Подробная идентификация связанного с аварийным сигналом ресурса, например, интерфейса или процесса.

Alarm Instance - экземпляр сигнала тревоги
Состояние сигнала тревоги для конкретного ресурса и сигнала, например, GigabitEthernet0/15, link-alarm. Это запись в списке аварийных сигналов.

Cleared Alarm - сброшенный сигнал тревоги
Сигнал тревоги, где система считает состояние нежелательным, сброшен. Оператор не может сбрасывать аварийные сигналы, за это отвечает система. Например, уведомление linkUp может считаться сбросом состояния linkDown.

Closed Alarm - закрытый сигнал тревоги
Операторы могут закрывать сигналы тревоги независимо от сброса сигнала. Закрытый сигнал указывает, что сигнал тревоги не требует внимания, поскольку были выполнены корректирующие действия или сигнал можно игнорировать по другим причинам.

Alarm Inventory - опись сигналов тревоги
Список всех возможных сигналов тревоги в системе.

Alarm Shelving - блокировка сигнала тревоги
Блокировка аварийных сигналов в соответствии с заданным критерием.

Corrective Action - корректировочное действие
Действие, предпринимаемое оператором или программой для минимизации влияния аварийного сигнала или устранения первопричины.

Management System - система управления
Приложение для управления сигналами тревоги, принимающего сигналы, например, клиент системы управления.

System - система

Система, реализующая модуль YANG, т. е. выступающая как сервер. Это сетевое устройство или управляющее приложение, обеспечивающее северный интерфейс для аварийных сигналов.

Деревья, представленные с этом документе, используют нотацию [RFC8340].

2. Цели

Цели разработки модели данных для аварийных сигналов перечислены ниже.

- Простота использования. Если система поддерживает этот модуль, её можно легко интегрировать в менеджер аварийных сигналов на основе YANG.
- Сигналы тревоги представляются как состояния ресурсов, а не дискретные уведомления.
- Представлено точное определение сигнала тревоги для исключения общих событий, которые не следует пересылать как уведомления о сигналах тревоги.
- Обеспечивается точная идентификация типов сигналов тревоги и их экземпляров.
- Системе управления следует поддерживать возможность опроса всех доступных в системе типов аварийных сигналов, т. е. считывания описи сигналов тревоги из системы. Это позвляте подготовить для операторов аварийных сигналов соответствующие инструкции.
- Выполнены требования при применимости аварийных сигналов (Приложение G. Требования к применимости аварийных сигналов). Хотя стандарты IETF и телекоммуникаций рассматривают аварийные сигналы в основном с точки зрения протоколов, в отрасли обработки имеется несколько опубликованных стандартов, касающихся требований к применимости интерфейса сигналов тревоги (см. [EEMUA] и [ISA182]). Этот документ задаёт требования применимости, а также модель данных YANG.
- Достижимо сопоставление с [X.733], требуемое для некоторых систем аварийной сигнализации. Тем не менее, некоторые концепции X.733 остаются за пределами базовой модели, чтобы сохранить простоту понимания и размер модели.

3. Концепции модели данных для аварийных сигналов

В этом разделе определены основные концепции модели данных на основе работы Vallin и др. [ALARMSEM].

3.1. Определение сигнала тревоги

Аварийный сигнал указывает нежелательное состояние ресурса системы, требующее корректирующих действий. Из этого определения следует запомнить два основных аспекта.

1. Основное внимание уделено исключению событий и записи информации в целом. Аварийные сигналы следует применять только для нежелательных сигналов, требующих действий.
2. Сигналы тревоги указывают состояние ресурса, а не являются уведомлением о смене состояния.

Связь этого определения со стандартами для аварийных сигналов описана в Приложении F.

3.2. Тип сигнала тревоги

Этот документ определяет тип сигналов тревоги с идентификатором и квалификатором alarm-type. Идентификатор alarm-type моделируется отождествлением YANG. С идетификаторами (отождествлениями) YANG можно определять новые типы сигналов тревоги распределенным способом. Идентификаторы YANG являются иерархическими, что позволяет определить иерахию аварийных сигналов. Производителям и органам стандартизации следует задавать свои отождествления alarm-type на основе этого определения.

Использование идентификаторов YANG означает, что все возможные аварийные сигналы идентифицированы во время разработки. Явное объявление типов аварийных сигналов упрощает квалификацию аварийных сигналов, подготовку действий по сигналам и документации.

Бывают случаи, когда типы аварийных сигналов неизвестны в момент разработки, например, система с цифровыми входами, позволяющая пользователям подключать датчики, такие как детекторы дыма.

Для возможности динамического добавления аварийных сигналов модель данных допускает дальнейшую классификацию основанных на идентификаторах типов аварийных сигналов в форме строк. Потенциальный недостаток этого заключается в существенном риске получения оператором неожиданных типов аварийных сигналов. Операторы не знают, как разрешить проблему, поскольку конкретной процедуры реагирования может не быть. Чтобы избежать такого риска система **должна** публиковать все возможные типы аварийных в описи сигналов (4.2. Опись сигналов тревоги).

Производители и органы стандартизации могут определять свою иерархию alarm-type. Ниже приведён пример иерархии на основе типов событий X.733.

```
import ietf-alarms {
  prefix al;
}
identity vendor-alarms {
  base al:alarm-type;
}
identity communications-alarm {
  base vendor-alarms;
}
identity link-alarm {
  base communications-alarm;
}
```

Типы аварийных сигналов могут быть абстрактными. Абстрактный тип служит базой для определения иарахии типов сигналов тревоги. Имеется два варианта конкретных типов аварийных сигналов.

1. Последний подчиненный идентификатор в иерархии alarm-type-id является конкретным, например, alarm-identity.environmental-alarm.smoke. В приведённом примере alarm-identity и environmental-alarm - абстрактные идентификаторы YANG, а smoke - конкретный.

2. Иерархия идентификаторов YANG является абстрактной, а конкретный тип задан динамической строкой alarm-qualifier, например, alarm-identity.environmental-alarm.external-detector с alarm-type-qualifier smoke.

Пример

```
// Вариант 1: конкретный идентификатор типа аварийного сигнала
import ietf-alarms {
  prefix al;
}
identity environmental-alarm {
  base al:alarm-type;
  description "Абстрактный тип сигнала.";
}
identity smoke {
  base environmental-alarm;
  description "Конкретный тип сигнала.";
}

// Вариант 2: конкретный классификатор типа аварийного сигнала
import ietf-alarms {
  prefix al;
}
identity environmental-alarm {
  base al:alarm-type;
  description "Абстрактный тип сигнала.";
}
identity external-detector {
  base environmental-alarm;
  description
    "Абстрактный тип сигнала. Процедура настройки в процессе
     работы задаёт тип обнаруженного сигнала, сообщаемый в
     alarm-type-qualifier.";
}
```

Серверу **следует** стремиться минимизировать число динамически определяемых типов сигналов тревоги.

3.3. Отождествление связанного с аварийным сигналом ресурса

Крайне важна возможность указать связанный с сигналом тревоги ресурс. Это указание должно быть максимально подробным. Если этот ресурс существует в дереве данных, **должен** использоваться идентификатор экземпляра с полным путём к объекту.

При использовании модуля в контроллере, оркестраторе или менеджере исходная идентификация ресурса может меняться для включения устройства в путь. Детали этого зависят от способа идентификации устройства и выходят за рамки этой спецификации.

Пример

Аварийный сигнал от устройства может указывать ресурс как /dev:interfaces/dev:interface[dev:name='FastEthernet1/0'], а в менеджере будет /mgr:devices/mgr:device[mgr:name='xyz123']/dev:interfaces/dev:interface[dev:name='FastEthernet1/0'].

Модуль также разрешает иное именование связанного с сигналом тревоги устройства, если его нет в дереве данных.

3.4. Идентификация экземпляров аварийных сигналов

Основной целью модели данных для сигналов тревоги является устранение неоднозначности сопоставления уведомления о сигнале с обновлением экземпляра аварийного сигнала. В X.733 [X.733] и 3GPP [ALARMIRP] на этот счёт нет ясности. В описываемой модели данных указано, что триплет (ресурс, идентификатор сигнала, классификатор сигнала) соответствует одному экземпляру сигнала тревоги. Это значит, что уведомления о сигнале тревоги для одного ресурса и одного типа сигнала сответствуют обновлению того же экземпляра. Эти три листа служат ключами списка сигналов тревоги.

```
list alarm {
  key "resource alarm-type-id alarm-type-qualifier";
  ...
}
```

3.5. Жизненный цикл сигнала тревоги

Модель сигналов тревоги чётко разделяет жизненные циклы сигнала в ресурсе, у оператора и административный.

- Жизненный цикл в ресурсе включет измерение, подающее сигнал, очистку и смену уровня важности.

- Жизненный цикл у оператора включает действия по сигналу, включая подтверждение и закрытие, котрое предполагает, что оператор считает корректирующие действия выполненными. Оператор может блокировать (игнорировать, фильтровать) сигналы для исключения ложных.

- Административный жизненный цикл включает очистку (удаление) нежелательных сигналов и сжатие списка изменений состояния сигналов тревоги. Модуль предоставляет операции для управления административным циклом. Сервер может выполнять эти операции на основе своих правил, но это выходит за рамки документа.

Серверу **следует** описывать, сколь долго он сохраняет сброшенные и закрытые сигналы, пока они не будут удалены вручную или по правилам автоматического удаления. Процедуры для этого выходят за рамки документа.

3.5.1. Жизненный цикл сигнала тревоги в ресурсе

С точки зрения ресурса аварийный согнал может иметь, например, цикл - активизация сигнала, смена важности, очистка, новая активизация и т. д. Для всех этих изменений статуса измерители генерируют разные сопровождающие тексты. Следует отметить два важных обстоятельства.

1. Сигналы не удаляются при очистке, удаление является административным процессом. В модуле YANG ietf-alarms задано действие purge-alarms для удаления сигналов тревоги.
2. Сигналы не очищаются оператором, это может сделать только измеритель. Оператор может закрыть сигнал.

Приведённое ниже представление дерева YANG иллюстрирует ориентированный на ресурсы жизненный цикл сигнала.

```
+--ro alarm* [resource alarm-type-id alarm-type-qualifier]
   ...
   +--ro is-cleared                boolean
   +--ro last-raised               yang:date-and-time
   +--ro last-changed              yang:date-and-time
   +--ro perceived-severity        severity
   +--ro alarm-text                alarm-text
   +--ro status-change* [time] {alarm-history}?
      +--ro time                   yang:date-and-time
      +--ro perceived-severity     severity-with-clear
      +--ro alarm-text             alarm-text
```

Для каждого изменения статуса с точки зрения ресурса в список status-change добавляется строка, если сервер реализует функцию alarm-history. Эта функция необязательна для реализации, поскольку сохранение истории аварийных сигналов может влиять на ресурсы памяти сервера.

Последние значения статуса представлены также как листья (leaf) для сигнала тревоги. Отметим, что важность сигнала не включает логического флага cleared.

Таким образом, аварийный сигнал может иметь вид (("GigabitEthernet0/25", "link-alarm",""), false, 2018-04-08T08:20:10.00Z, 2018-04-08T08:20:10.00Z, major, "Interface GigabitEthernet0/25 down").

3.5.2. Жизненный цикл сигнала тревоги у оператора

Операторы могут применять к сигналам тревоги действие set-operator-state.

```
+--ro alarm* [resource alarm-type-id alarm-type-qualifier]
   ...
   +--ro operator-state-change* [time] {operator-actions}?
   |  +--ro time        yang:date-and-time
   |  +--ro operator    string
   |  +--ro state       operator-state
   |  +--ro text?       string
   +---x set-operator-state {operator-actions}?
      +---w input
         +---w state    writable-operator-state
         +---w text?    string
```

Операторским состоянием для сигнала тревоги может быть none, ack, shelved, closed. Удаление сигнала (действие purge-alarms) может использовать статус сигнала в качестве критерия. Например, закрытым считается сигнал тревоги, для которого оператор выполнил все требуемые действия по исправлению ситуации, поэтому такие сигналы можно очищать (purge).

3.5.3. Административный жизненный цикл сигнала тревоги

Удаление сигналов тревоги из списка считается административным действием purge-alarms, принимающим на входе выражение для фильтра. Фильтр указывает аварийные сигналы на основе жизненного цикла у оператора и в ресурсе, такие как «все сигналы до указанного момента». Сервер также может выполнять операции на основе других правил, но это выходит за рамки документа.

Очищенные сигналы тревоги удаляются из списка. Отметим, что при изменении состояния связанного с сигналом ресурса изменится после очистки, сигнал может снова появиться в списке.

Сигналы тревоги можно сжимать. При этом удаляются все записи списка status-change, кроме последней смены состояния. Клиент может выполнить сжатие с помощью действия compress-alarms. Сервер может выполнять сжатие на основе других правил, но это выходит за рамки документа.

3.6. Первопричина, затронутые ресурсы и сигналы тревоги

Модель данных сигналов тревоги не предъявляет к системе требований по поддержке сопоставлений аварийных сигналов и анализа первопричин или влияния на службы. Однако для случаев поддержки таких функций этот параграф описывает представление такого анализа в модели данных. Эти части модели являются необязательными. Модуль поддерживает три сценария.

Root-cause analysis - анализ первопричины
: Сигнал может указывать ресурсы, которые могут быть первопричиной, например, сигнал базы данных о заполнении дискового раздела.

Service-impact analysis - анализ влияния на службы
: Сигнал может относиться к затрагиваемым ресурсам, например, аварийный сигнал сетевого интерфейса может говорить о влиянии на сетевые службы.

Alarm correlation - сопоставление аварийных сигналов

Между сигналами могут быть зависимости. Несколько сигналов могут группироваться, например, сигнал потоковой среды, связанный с сигналом о значительных вариациях задержки (high-jitter).

Системы различаются по способности сопоставления и анализа сигналов тревоги и назначение модели данных состоит в том, чтобы поддерживать любую возможность, в том числе их отсутствие.

Общим принципом этой модели данных является сокращение числа аварийных сигналов. Во многих случаях одна базовая проблема воздействует на несколько ресурсов. Например, заполнение диска влияет на базы данных и приложения. Рекомендуется иметь один сигнал тревоги для базовой проблемы и список затрагиваемых ею ресурсов, а не раздельные аварийные сигналы для каждого ресурса.

Аварийный сигнал имеет leaf-list для указания возможного impacted-resource и leaf-list для возможного root-cause-resource, которые служат лишь советами. Клиентское приложение может использовать эти сведения для представления общего состояния. В примере с заполненным диском хорошим сигналом будет указание раздела диска в качестве связанного с сигналом ресурса и добавление базы данных и приложений в лист-список impacted-resource.

Системе следует стремиться указать ресурс, на который можно воздействовать, как лист resource. Лист-список impacted-resource нужно использовать для указания побочных влияний сигнала тревоги, поскольку воздействие на эти ресурсы не поможет в решении проблемы. В примере с заполненным диском иллюстрируется этот принцип - проблему невозможно решить с помощью операций базы данных, однако нужно обратить на неё внимание при выполнении операций, ограничивающих влияние проблемы.

В некоторых ситуациях система может быть не способна выявить первопричину - ресурс, на который нужно воздействовать. Измерения в этом случае лишь отслеживают побочные эффекты и выдают сигнал тревоги для указания ситуации, требующей внимания, и могут определить кандидатов на роль ресурса, являющегося первопричиной. В этом случае можно использовать лист-список root-cause-resource для указания таких кандидатов. Примером такого рода сигнала может быть активный инструмент тестирования, который обнаруживает нарушение соглашения об уровне обслуживания (Service Level Agreement или SLA) для соединения VPN и указывает устройства в цепочке, как возможные первопричины.

Модель данных сигналов тревоги поддерживает возможность группировать связанные сигналы в списке related-alarm. Это позволяет серверу информировать клиента о наличии связей между аварийными сигналами.

Отметим, что модуль не предписывает каких-либо зависимостей или предпочтений среди упомянутых механизмов сопоставления аварийных сигналов. Возможности систем различаются и описанные выше механизмы доступны для инструментальных функций.

3.7. Блокировка аварийных сигналов

Блокировка (shelving) аварийных сигналов является важной функцией, позволяющей приложениям управления сигналами тревоги и операторам исключить лишние сигналы, путём их игнорирования (блокировки, фильтрации). Игнорируемые сигналы указываются в специальном списке shelved-alarm, позволяющем отфильтровать их, оставляя в основном списке сигналов лишь интересующие записи. Заблокированные сигналы порождают уведомлений, но список shelved-alarm обновляется при любых изменениях состояния сигналов (alarm-state).

Блокировку сигналов тревоги необязательно реализовать, поскольку сопоставление сигналов тревоги с критериями блокировки может влиять на серверные ресурсы обработки.

3.8. Профили аварийных сигналов

Профили аварийных сигналов служат для настройки дополнительных сведений о типе сигнала. Этот модуль поддерживает уровни важности, переопределяющие принятые в системе по умолчанию. Это соответствует функциональности профиля назначения важности сигналов тревоги (Alarm Severity Assignment Profile или ASAP) в M.3100 [M.3100] и M.3160 [M.3160]. Другие стандартные или фирменные модули могут дополнять список сведениями о типах сигналов тревоги.

4. Модель данных

Основными частями модели данных являются список аварийных сигналов alarm-list со связанными уведомлениями и список alarm-inventory со всеми типами возможных сигналов тревоги, которые **должны** быть реализованы в системе. Остальная часть модели сделана условной с помощью функций YANG (feature) operator-actions, alarm-shelving, alarm-history, alarm-summary, alarm-profile, severity-assignment. Общая структура модели данных приведена ниже.

```
+--rw control
|  +--rw max-alarm-status-changes?   union
|  +--rw notify-status-changes?      enumeration
|  +--rw notify-severity-level?      severity
|  +--rw alarm-shelving {alarm-shelving}?
|        ...
+--ro alarm-inventory
|  +--ro alarm-type* [alarm-type-id alarm-type-qualifier]
|        ...
+--ro summary {alarm-summary}?
|  +--ro alarm-summary* [severity]
|  |     ...
|  +--ro shelves-active?   empty {alarm-shelving}?
+--ro alarm-list
|  +--ro number-of-alarms?   yang:gauge32
|  +--ro last-changed?       yang:date-and-time
|  +--ro alarm* [resource alarm-type-id alarm-type-qualifier]
|  |     ...
|  +---x purge-alarms
|  |     ...
|  +---x compress-alarms {alarm-history}?
```

```
|        ...
+--ro shelved-alarms {alarm-shelving}?
|  +--ro number-of-shelved-alarms?      yang:gauge32
|  +--ro shelved-alarms-last-changed?   yang:date-and-time
|  +--ro shelved-alarm*
|  |       [resource alarm-type-id alarm-type-qualifier]
|  |     ...
|  +---x purge-shelved-alarms
|  |     ...
|  +---x compress-shelved-alarms {alarm-history}?
|        ...
+--rw alarm-profile*
         [alarm-type-id alarm-type-qualifier-match resource]
         {alarm-profile}?
   +--rw alarm-type-id                        alarm-type-id
   +--rw alarm-type-qualifier-match           string
   +--rw resource                             resource-match
   +--rw description                          string
   +--rw alarm-severity-assignment-profile
           {severity-assignment}?
         ...
```

4.1. Управление аварийными сигналами

Лист /alarms/control/notify-status-changes указывает, следует передавать уведомления для любой смены состояния, только для активации, только для очистки или только при превышении заданного уровня важности. Эта функция в сочетании с блокировкой сигналов тревоги соответствует функциям ITU Alarm Report Control (Приложение F.2.4).

Каждый сигнал тревоги имеет список смены состояний. Размер этого списка задает /alarms/control/max-alarm-status-changes. При заполненном списке создание новой записи удаляет самую старую.

4.1.1. Блокирование сигналов тревоги

Ниже показано дерево управления блокировкой сигналов тревоги.

```
+--rw control
   +--rw alarm-shelving {alarm-shelving}?
      +--rw shelf* [name]
         +--rw name            string
         +--rw resource*       resource-match
         +--rw alarm-type*
         |       [alarm-type-id alarm-type-qualifier-match]
         |  +--rw alarm-type-id                 alarm-type-id
         |  +--rw alarm-type-qualifier-match    string
         +--rw description?    string
```

Заблокированные сигналы указываются в отдельном списке shelved-alarm. Соответствующие сигналы тревоги **должны** указываться в списке /alarms/shelved-alarms/shelved-alarm, а прочие **должны** помещаться в /alarms/alarm-list/alarm. Сервер не передаёт уведомлений для заблокированных сигналов.

Установка и снятие блокировки выполняются только редактированием конфигурации блокировки и невозможны для отдельного сигнала тревоги. Сервер добавляет состояние у оператора, связанное с блокировкой сигналов тревоги.

Лист /alarms/summary/shelves-active в сводке сигналов тревоги указывает, были ли сигналы экранированы.

Система не обязана поддерживать функцию экранирования.

4.2. Опись сигналов тревоги

Опись (inventory) аварийных сигналов представляет все типы сигналов тревоги, возможных в системе. Система управления может применять этот список для организации процедур обработки. Причины актуальности описи сигналов указаны ниже.

- Ссистема может не реализовать все указанные идентификаторы типов сигналов тревоги, а некоторые идентификаторы являются абстрактными.
- В системе настроены динамические типы сигналов с использованием классификаторов. Опись позволяет системе управления найти такие типы.

Отметим, что механизм добавления динамических типов сигналов **должен** добавлять их в эту опись.

Необязательный лист resource в описи аварийных сигналов позволяет системе публиковать сведения о ресурсах, к которым может относиться данный тип сигналов тревоги.

Сервер **должен** реализовать опись аварийных сигналов для поддержки управляемых процедур обработки у клиентов.

Разработчики сервера могут документировать опись аварийных сигналов для автономной обработки клиентами. Для этого можно использовать формат файла из [YANG-INSTANCE]. Ниже приведено дерево описи аварийных сигналов.

```
+--ro alarm-inventory
   +--ro alarm-type* [alarm-type-id alarm-type-qualifier]
      +--ro alarm-type-id           alarm-type-id
      +--ro alarm-type-qualifier    alarm-type-qualifier
      +--ro resource*               resource-match
      +--ro will-clear              boolean
      +--ro severity-level*         severity
      +--ro description             string
```

4.3. Сводка сигналов тревоги

В сводном списке содержатся аварийные сигналы по их важности - число очищенных, очищенных и закрытых, закрытых. Указывается также наличие заблокированных сигналов. Дерево сводного списка сигналов приведено ниже.

```
  +--ro summary {alarm-summary}?
     +--ro alarm-summary* [severity]
     |  +--ro severity                  severity
     |  +--ro total?                    yang:gauge32
     |  +--ro not-cleared?              yang:gauge32
     |  +--ro cleared?                  yang:gauge32
     |  +--ro cleared-not-closed?       yang:gauge32
     |  |       {operator-actions}?
     |  +--ro cleared-closed?           yang:gauge32
     |  |       {operator-actions}?
     |  +--ro not-cleared-closed?       yang:gauge32
     |  |       {operator-actions}?
     |  +--ro not-cleared-not-closed?   yang:gauge32
     |          {operator-actions}?
     +--ro shelves-active?   empty {alarm-shelving}?
```

4.4. Список аварийных сигналов

Список сигналов тревоги /alarms/alarm-list является функцией от тройки (resource, alarm type, alarm-type qualifier) до текущего состояния сигнала. Композитное состояние включает состояния жизненного цикла сигнала в ресурсе, флага очистки и состояния у оператора, такие как подтверждения. Это означает, что для данного ресурса и типа сигнала список показывает текущие состояния сигналов тревоги, такие как подтверждение и очистка.

```
+--ro alarm-list
   +--ro number-of-alarms?   yang:gauge32
   +--ro last-changed?       yang:date-and-time
   +--ro alarm* [resource alarm-type-id alarm-type-qualifier]
   |  +--ro resource                 resource
   |  +--ro alarm-type-id            alarm-type-id
   |  +--ro alarm-type-qualifier     alarm-type-qualifier
   |  +--ro alt-resource*            resource
   |  +--ro related-alarm*
   |  |       [resource alarm-type-id alarm-type-qualifier]
   |  |       {alarm-correlation}?
   |  |  +--ro resource
   |  |  |       -> /alarms/alarm-list/alarm/resource
   |  |  +--ro alarm-type-id           leafref
   |  |  +--ro alarm-type-qualifier    leafref
   |  +--ro impacted-resource*       resource
   |  |       {service-impact-analysis}?
   |  +--ro root-cause-resource*     resource
   |  |       {root-cause-analysis}?
   |  +--ro time-created             yang:date-and-time
   |  +--ro is-cleared               boolean
   |  +--ro last-raised              yang:date-and-time
   |  +--ro last-changed             yang:date-and-time
   |  +--ro perceived-severity       severity
   |  +--ro alarm-text               alarm-text
   |  +--ro status-change* [time] {alarm-history}?
   |  |  +--ro time                  yang:date-and-time
   |  |  +--ro perceived-severity    severity-with-clear
   |  |  +--ro alarm-text            alarm-text
   |  +--ro operator-state-change* [time] {operator-actions}?
   |  |  +--ro time        yang:date-and-time
   |  |  +--ro operator    string
   |  |  +--ro state       operator-state
   |  |  +--ro text?       string
   |  +---x set-operator-state {operator-actions}?
   |  |  +---w input
   |  |     +---w state    writable-operator-state
   |  |     +---w text?    string
   |  +---n operator-action {operator-actions}?
   |     +-- time        yang:date-and-time
   |     +-- operator    string
   |     +-- state       operator-state
   |     +-- text?       string
   +---x purge-alarms
   |  +---w input
   |  |  +---w alarm-clearance-status    enumeration
   |  |  +---w older-than!
   |  |  |  +---w (age-spec)?
   |  |  |     +--:(seconds)
   |  |  |     |  +---w seconds?   uint16
   |  |  |     +--:(minutes)
   |  |  |     |  +---w minutes?   uint16
   |  |  |     +--:(hours)
   |  |  |     |  +---w hours?     uint16
   |  |  |     +--:(days)
   |  |  |     |  +---w days?      uint16
   |  |  |     +--:(weeks)
   |  |  |        +---w weeks?     uint16
   |  |  +---w severity!
```

```
|  |  |  +---w (sev-spec)?
|  |  |     +--:(below)
|  |  |     |  +---w below?   severity
|  |  |     +--:(is)
|  |  |     |  +---w is?      severity
|  |  |     +--:(above)
|  |  |        +---w above?   severity
|  |  +---w operator-state-filter! {operator-actions}?
|  |     +---w state?   operator-state
|  |     +---w user?    string
|  +--ro output
|     +--ro purged-alarms?   uint32
+---x compress-alarms {alarm-history}?
   +---w input
   |  +---w resource?               resource-match
   |  +---w alarm-type-id?
   |  |       -> /alarms/alarm-list/alarm/alarm-type-id
   |  +---w alarm-type-qualifier?   leafref
   +--ro output
      +--ro compressed-alarms?   uint32
```

У каждого аварийного сигнала есть три важных состояния - очистка для ресурса is-cleared, воспринимаемый уровень важности perceived-severity и состояние оператора, доступное в списке operator-state.

История сигналов тревоги для смены состояний в ресурсах хранится в списке status-change, а история состояний у оператора - в списке operator-state-change.

4.5. Список заблокированных сигналов

Структура списка shelved-alarm совпадает с описанной выше. Он содержит аварийные сигналы, соответствующие критерию блокировки из /alarms/control/alarm-shelving.

4.6. Профили сигналов

Профиль аварийных сигналов /alarms/alarm-profile является списком настраиваемых типов сигналов тревоги. Этот список поддерживает указание уровней важности в контейнере alarm-severity-assignment-profile. Если аварийный сигнал соответствует настроенному типу, он **должен** использовать заданный уровень важности вместо принятого в системе по умолчанию. Конфигурация **должна** также представляться в сводке аварийных сигналов.

```
+--rw alarm-profile*
        [alarm-type-id alarm-type-qualifier-match resource]
        {alarm-profile}?
   +--rw alarm-type-id                        alarm-type-id
   +--rw alarm-type-qualifier-match           string
   +--rw resource                             resource-match
   +--rw description                          string
   +--rw alarm-severity-assignment-profile
           {severity-assignment}?
      +--rw severity-level*    severity
```

4.7. Операции

Модель данных для сигналов тревоги поддерживает указанные ниже действия для управления этими сигналами.

/alarms/alarm-list/purge-alarms
: Удаление сигналов из alarm-list по заданному критерию, например, все сброшенные сигналы до указанной даты.

/alarms/alarm-list/compress-alarms
: Сжатие списка аварийных сигналов status-change.

/alarms/alarm-list/alarm/set-operator-state
: Смена состояния сигнала у оператора, например, сигнал можно подтвердить, установив статус ack.

/alarms/shelved-alarm-list/purge-shelved-alarms
: Удаление сигналов из shelved-alarm-list по заданному критерию, например, все сброшенные сигналы до указанной даты.

/alarms/shelved-alarm-list/compress-shelved-alarms
: Сжатие списка status-change для аварийных сигналов.

4.8. Уведомления

Модель данных для сигналов тревоги поддерживает базовое уведомление о смене статуса - alarm-state. Оно включает параметры, нужные приложениям, работающим с аварийными сигналами.

Имеется также уведомление для информирования смены оператором статуса сигнала, например, о подтверждении.

При смене сводки сигналов тревоги, например, вставке платы нового типа, уведомление будет информировать управляющие приложения о доступности нового типа сигналов тревоги.

5. Связь с модулем YANG ietf-hardware

В RFC 8348 [RFC8348] задан модуль YANG ietf-hardware для управления оборудованием. Узел alarm-state в RFC 8348 содержит сводку уровней важности, которые могут быть активны для соответствующего оборудования, но ничего не говорит о способах информирования при авариях и не включает деталей аварийных сигналов.

Ниже показано сопоставление префикса al в этой модели данных и с alarm-state и префиксом hw в RFC 8348.

al:resource
: Соответствует записи списка /hw:hardware/hw:component/.

al:is-cleared

Бит в /hw:hardware/hw:component/hw:state/hw:alarm-state не установлен.

al:perceived-severity

Соответствующий бит в /hw:hardware/hw:component/hw:state/hw:alarm-state установлен.

al:operator-state-change/al:state

Если сигнал подтверждён оператором, устанавливается бит hw:under-repair в /hw:hardware/hw:component/hw:state/hw:alarm-state.

6. Модуль YANG для сигналов тревоги

Этот модуль YANG ссылается на [RFC6991] и [XSD-TYPES].

```
<CODE BEGINS> file "ietf-alarms@2019-09-11.yang"
module ietf-alarms {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-alarms";
  prefix al;

  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types.";
  }

  organization
    "IETF CCAMP Working Group";
  contact
    "WG Web:   <https://trac.ietf.org/trac/ccamp>
     WG List:  <mailto:ccamp@ietf.org>

     Editor:   Stefan Vallin
               <mailto:stefan@wallan.se>

     Editor:   Martin Bjorklund
               <mailto:mbj@tail-f.com>";
  description
    "Этот модуль задаёт интерфейс для управления сигналами тревоги.
     Основными источниками для создания модуля послужили стандарты
     3GPP Alarm IRP, ITU-T X.733, ANSI/ISA-18.2.

     Основные функции модуля указаны ниже.
       * Список аварийных сигналов. Сброшенные сигналы остаются в
         списке, пока не будут явно очищены.
       * Действия оператора по сигналу - подтверждение и закрытие.
       * Административные действия по сигналы - очистка списка
         сигналов в соответствии с конкретными критериями.
       * Опись сигналов - управляющее приложение может считывать все
         сигналы, реализованные системой.
       * Блокировка (экранирование) сигналов в соответствии с
         конкретными критериями.
       * Профили сигналов. Система управления может связывать с типом
         сигнала дополнительные сведения, например, переопределять
         принятый по умолчанию в системе уровень важности.

     Этот модуль использует представление аварийных сигналов с учётом
     состояния. Сигнал является состоянием конкретного ресурса
     (отметим, что сигнал не является уведомлением). Типом сигнала
     является возможное состояние сигнала для ресурса. Например,
             ('link-alarm', 'GigabitEthernet0/25')
     является сигналом типа link-alarm на ресурсе GigabitEthernet0/25.

     Типы сигналов тревоги указываются идентификаторами YANG и
     необязательными строковыми классификаторами, которые позволяют
     динамически расширять статический набор типов сигналов. Типы
     сигналов указывают возможное состояние тревоги, а не отдельные
     уведомления. Например, традиционные уведомления link-down и
     link-up относятся к одному типу аварийных сигналов (link-alarm).

     При таком устройстве не возникает неоднозначности сопоставления
     аварийных сигналов и их сброса. Уведомления для одного ресурса и
     типа сигнала считаются обновлениями одного сигнала, например,
     очисткой активного сигнала или сменой уровня важности. Измерения
     могут менять уровень важности и текст имеющегося аварийного
     сигнала. Упомянутый выше пример сигнала может иметь вид
     example can therefore look like the following:

       (('link-alarm', 'GigabitEthernet0/25'), warning,
        'interface down while interface admin state is up')

     Чётко отделено обновление сигнала тревоги от базового ресурса,
     подобно очистке и обновлениям от оператора, например, при
     подтверждении или закрытии аварийного сигнала
       (('link-alarm', 'GigabitEthernet0/25'), warning,
        'interface down while interface admin state is up', cleared,
        closed)
```

```
      Поддерживаются административные действия, такие как удаление
      закрытых сигналов тревоги старше указанного возраста.

      Этот модуль YANG не задаёт обнаружение и сброс конкретных
      сигналов тревоги средствами измерения. Этот вопрос решают органы
      стандартизации (SDO) и предприятия, владеющие технологией.

      Ключевые слова ДОЛЖНО, НЕДОПУСТИМО, ТРЕБУЕТСЯ, НУЖНО, НЕ НУЖНО,
      СЛЕДУЕТ, НЕ СЛЕДУЕТ, РЕКОМЕНДУЕТСЯ, НЕ РЕКОМЕНДУЕТСЯ, МОЖНО,
      НЕОБЯЗАТЕЛЬНО в этом документе трактуются в соответствии с
      BCP 14 (RFC 2119) (RFC 8174) тогда и только тогда, когда они
      указаны заглавными буквами, как показано здесь.

      Авторские права (Copyright (c) 2019) принадлежат IETF Trust и
      лицам, указанным как авторы. Все права защищены.

      Распространение и применение модуля в исходной или двоичной
      форме с изменениями или без таковых разрешено в соответствии с
      лицензией Simplified BSD License, изложенной в параграфе 4.c
      IETF Trust's Legal Provisions Relating to IETF Documents
      (https://trustee.ietf.org/license-info).

      Эта версия модуля YANG является частью RFC 8632, где правовые
      аспекты приведены более полно.";

    revision 2019-09-11 {
      description
        "Исходный выпуск.";
      reference
        "RFC 8632: A YANG Data Model for Alarm Management";
    }

    /*
     * Свойства (функции)
     */

    feature operator-actions {
      description
        "Указывает, что система поддерживает состояния аварийных
         сигналов у оператора.";
    }

    feature alarm-shelving {
      description
        "Указывает, что система поддерживает блокировку сигналов.
         Блокировка может влиять на ресурсы обработки на сервере
         из-за сопоставления сигналов с критериями блокировки.";
    }

    feature alarm-history {
      description
        "Указывает, что сервер поддерживает историю смены состояний для
         каждого аварийного сигнала. Например, при 10-кратных переходах
         между cleared и active это будет представлено отдельным списком
         для аварийного сигнала. Сохранение истории может влиять на
         используемые сервером ресурсы памяти.";
    }

    feature alarm-summary {
      description
        "Указывает, что сервер поддерживает сводку аварийных сигналов по
         уровню важности и состоянию у оператора.";
    }

    feature alarm-profile {
      description
        "Система позволяет клиентам настраивать дополнительную
         информацию для каждого типа сигналов тревоги.";
    }

    feature severity-assignment {
      description
        "Система поддерживает настраиваемые уровни важности сигналов.";
      reference
        "ITU-T Recommendation M.3100:
           Generic network information model
         ITU-T Recommendation M.3160:
           Generic, protocol-neutral management information model";
    }

    feature root-cause-analysis {
      description
        "Система поддерживает идентификацию ресурсов-кандидатов для
         первопричины сигнала тревоги, например, дисковый раздел для
         сигнала об отказе регистрации в системном журнале.";
    }
```

```
feature service-impact-analysis {
  description
    "Система поддерживает идентификацию ресурсов, которые могут
     быть затронуты аварийным сигналом, например, смена состояния
     канала может указывать воздействие на канал.";
}

feature alarm-correlation {
  description
    "Система поддерживает сопоставление и группировку сигналов.";
}

/*
 * Идентификаторы (отождествления)
 */

identity alarm-type-id {
  description
    "Базовый идентификатор типа аварийного сигнала, однозначно
     указывающий сигнал тревоги без указания ресурса. Один тип
     может относится к разным ресурсам. Если ресурс сообщает один и
     тот же тип сигнала, это считается тем же сигналом. Тип сигнала
     является упрощением различных механизмов сопоставления X.733 и
     3GPP Alarm IRP и допускает иерархическое расширение.

     К идентификатору может добавляться строковый классификатор,
     чтобы различать типы аварийных сигналов на основе сведений,
     неизвестных в момент разработки, таких как значения в тексте
     привязок переменных SNMP Notification.

     Стандарты и производители могут задавать субидентификаторы
     для указания конкретных типов аварийных сигналов.

     Этот идентификатор является абстракцией и его НЕДОПУСТИМО
     применять для конкретных сигналов тревоги.";
}

/*
 * Базовые типы
 */

typedef resource {
  type union {
    type instance-identifier {
      require-instance false;
    }
    type yang:object-identifier;
    type string;
    type yang:uuid;
  }
  description
    "Это указание ресурса, с которым связан сигнал тревоги, такого
     как интерфейс. Это указание следует делать подробным, чтобы
     направить оператора и обеспечить уникальность сигналов.

     Если затронутый интерфейс моделируется в YANG, это может быть
     instance-identifier. Если ресурс является объектом SNMP, типом
     будет object-identifier. Для прочих ресурсов, например,
     отличительного пути в базовой информационной модели (Common
     Information Model или CIM) этот тип будет строкой.

     Если связанный с сигналом ресурс указан UUID, применяется тип
     uuid. Этот тип следует применять с осторожностью, поскольку
     оператору сложно работать со значениями UUID.

     Если сервер поддерживает несколько моделей, следует применять
     предпочтения в порядке из определения объединения (union).";
}

typedef resource-match {
  type union {
    type yang:xpath1.0;
    type yang:object-identifier;
    type string;
  }
  description
    "Этот тип служит для сопоставления ресурса с типом resource.
     Поскольку тип resource является объединением (union) разных
     типов, resource-match будет объединением соответствующих типов.

     Если тип задан выражением XPath 1.0, ресурс типа
     instance-identifier будет соответствовать, когда экземпляр
     входит в набор узлов, заданный выражением XPath 1.0. Например,
      /ietf-interfaces:interfaces/ietf-interfaces:interface
          [ietf-interfaces:type='ianaift:ethernetCsmacd']
```

```
        будет соответствовать ресурсу instance-identifier
         /if:interfaces/if:interface[if:name='eth1'],
        при условии, что eth1 имеет тип ianaift:ethernetCsmacd.

        Если тип задан идентификатором объекта, ресурс типа
        object-identifier будет соответствовать, когда идентификатор
        объекта является префиксом идентификатора объекта для ресурса
        Например, значению 1.3.6.1.2.1.2.2 будет соответствовать
        идентификатор ресурса 1.3.6.1.2.1.2.2.1.1.5.

        Если тип задан UUID или строкой, он интерпретируется как
        регулярное выражение XML Schema, которому соответствует ресурс
        типа yang:uuid или string при соответствии регулярного
        выражения строке ресурса.

        Если тип задан выражением XPath, оно оценивается в описанном
        ниже контексте XPath
          -  Набором объявлений пространств имён служит набор пар
             (префикс, пространство имён) для всех модулей YANG,
             реализованных сервером, где префиксом является имя модуля
             YANG, а пространство имён определяет оператор namespace в
             модуле YANG.
             Если лист этого типа кодируется в XML, все объявления
             пространств имён в области действия листа добавляются в
             набор объявлений пространств имён. Если найденный в XML
             префикс уже имеется в наборе объявлений, используется
             пространство имён в XML.
          -  Набор привязок переменных пуст.
          -  Библиотекой функций является библиотека функций ядра
             и функции заданы в разделе 10 RFC 7950.
          -  Узлом контекста является корень дерева данных.";
    reference
      "XML Schema Part 2: Datatypes Second Edition,
         World Wide Web Consortium Recommendation
         REC-xmlschema-2-20041028";
  }

  typedef alarm-text {
    type string;
    description
      "Строка для информирования оператора о сигнале тревоги, которая
       ДОЛЖНА содержать сведения, позволяющие оператору понять и
       устранить проблему. Если строка имеет структуру, она должна
       быть чётко документирована, чтобы информацию можно было
       проанализировать.";
  }

  typedef severity {
    type enumeration {
      enum indeterminate {
        value 2;
        description
          "Уровень важности не удаётся определить. СЛЕДУЕТ избегать
           этого значения.";
      }
      enum warning {
        value 3;
        description
          "Уровень warning (предупреждение) показывает обнаружение
           потенциальной или предстоящей неполадки до того, как будут
           ощутимы значимые последствия. Следует принять меры для
           дальнейшей диагностики (при необходимости) и устранения
           проблемы, чтобы не возникло более серьёзных неполадок,
           влияющих на службы.";
      }
      enum minor {
        value 4;
        description
          "Уровень minor (незначительный) указывает наличие отказа,
           не влияющего на службы. Следует принять меры предотвращения
           более серьёзного отказа (например, влияющего на службы).
           Такой уровень можно указывать, например, при обнаружении
           условий, которые пока не сокращают возможности ресурса.";
      }
      enum major {
        value 5;
        description
          "Уровень major (важный) указывает условия, влияющие на
           службы и требующие срочного исправления. Такой уровень
           может указываться при серьёзном ухудшении возможностей
           ресурса, когда требуется восстановление работоспособности";
      }
      enum critical {
        value 6;
        description
          "Уровень critical (критический) указывает серьёзное влияние
```

```
            на сервис, требующее немедленных действий по исправлению.
            Такой уровень может указываться, когда ресурс не способен
            работать и требует быстрого восстановления.";
        }
      }
      description
        "Уровень важности сигнала тревоги. Отметим, что значение clear
         не включено. Очистка сигнала указывается логическим флагом.";
      reference
        "ITU-T Recommendation X.733: Information Technology
           - Open Systems Interconnection
           - System Management: Alarm Reporting Function";
    }

    typedef severity-with-clear {
      type union {
        type enumeration {
          enum cleared {
            value 1;
            description
              "Сигнал очищен административно.";
          }
        }
        type severity;
      }
      description
        "Уровень важности сигнала с включением очистки. Применяется лишь
         в уведомлениях о смене состояний аварийных сигналов.";
    }

    typedef writable-operator-state {
      type enumeration {
        enum none {
          value 1;
          description
            "За сигналом не следят.";
        }
        enum ack {
          value 2;
          description
            "За сигналом наблюдают, корректирующие действия не
             выполнялись или завершились отказом";
        }
        enum closed {
          value 3;
          description
            "Корректирующие действия успешны.";
        }
      }
      description
        "Сообщение оператора о сигнале. Состояние closed указывает, что
         оператор считает тревогу устранённой. Это отделено от листа
         is-cleared для сигнала тревоги.";
    }

    typedef operator-state {
      type union {
        type writable-operator-state;
        type enumeration {
          enum shelved {
            value 4;
            description
              "Сигнал блокируется. Сигналам в /alarms/shelved-alarms/
               сервер ДОЛЖЕН назначать это состояние у оператора как
               последнюю запись в списке operator-state-change. В текст
               этой записи СЛЕДУЕТ включать имя блокировки.";
          }
          enum un-shelved {
            value 5;
            description
              "Сигнал возвращён в alarm-list после блокировки. Сигналам,
               перенесенным из /alarms/shelved-alarms/ в
               /alarms/alarm-list, сервер ДОЛЖЕН назначать этот статус
               как последнюю запись в списке operator-state-change. В
               текст записи СЛЕДУЕТ включать имя блокировки.";
          }
        }
      }
      description
        "Состояния сигнала у оператора. Статус closed показывает, что
         оператор считает проблему решённой. Это отличается от листа
         is-cleared для аварийного сигнала.";
    }

    /* Типы сигналов тревоги */
```

```
  typedef alarm-type-id {
    type identityref {
      base alarm-type-id;
    }
    description
      "Идентификатор типа сигнала тревоги. Описание идентификатора
       ДОЛЖНО указывать, является ли этот тип абстрактным. Абстрактные
       типы служат базой для остальных и не применяются как значения
       сигналов и не включаются в сводку сигналов тревоги.";
  }

  typedef alarm-type-qualifier {
    type string;
    description
      "Если сигнал не может быть полностью задан во время разработки
       значением alarm-type-id, этот строковый классификатор служит
       для полного определения уникального типа аварийного сигнала.

       Определение классификаторов сигналов считается частью измерения
       и выходит за рамки этого модуля. При использовании как части
       ключа, указывается пустая строка.";
  }

  /*
   * Группировки
   */

  grouping common-alarm-parameters {
    description
      "Базовые параметры сигнала тревоги. Эта группа применяется в
       списке сигналов и уведомлениях о смене alarm-state.";
    leaf resource {
      type resource;
      mandatory true;
      description
        "Связанный с сигналом тревоги ресурс, см. также alt-resource.
         Это может быть, например, ссылка на интерфейс с аварией";
    }
    leaf alarm-type-id {
      type alarm-type-id;
      mandatory true;
      description
        "Этот лист вместе с alarm-type-qualifier обеспечивает
         однозначное указание типа аварийного сигнала.";
    }
    leaf alarm-type-qualifier {
      type alarm-type-qualifier;
      description
        "Этот лист применяется, когда alarm-type-id не может
         однозначно указать тип сигнала. Обычно это не так и лист
         является пустой строкой.";
    }
    leaf-list alt-resource {
      type resource;
      description
        "Используется при доступности вызвавшего тревогу ресурса через
         другие интерфейсы. Поле может содержать SNMP OID, пути CIM,
         отличительные имена 3GPP и др.";
    }
    list related-alarm {
      if-feature "alarm-correlation";
      key "resource alarm-type-id alarm-type-qualifier";
      description
        "Указывает связанные сигналы тревоги. Отметим, что связанный
         сигнал может быть удалён из списка сигналов тревоги.";
      leaf resource {
        type leafref {
          path "/alarms/alarm-list/alarm/resource";
          require-instance false;
        }
        description
          "Связанный с тревогой ресурс для аварийного сигнала.";
      }
      leaf alarm-type-id {
        type leafref {
          path "/alarms/alarm-list/alarm"
             + "[resource=current()/../resource]"
             + "/alarm-type-id";
          require-instance false;
        }
        description
          "Идентификатор типа сигнала тревоги.";
      }
      leaf alarm-type-qualifier {
        type leafref {
          path "/alarms/alarm-list/alarm"
```

```
            + "[resource=current()/../resource]"
            + "[alarm-type-id=current()/../alarm-type-id]"
            + "/alarm-type-qualifier";
          require-instance false;
        }
        description
          "Классификатор для сигнала тревоги.";
      }
    }
    leaf-list impacted-resource {
      if-feature "service-impact-analysis";
      type resource;
      description
        "Ресурсы, на которые может влиять этот сигнал. Если система
         создаёт сигнал для ресурса и сопоставляет его с ресурсами, на
         которые сигнал может влиять, такие ресурсы могут быть указаны
         здесь. За счёт этого система может создавать один аварийный
         сигнал вместо нескольких. Например, при возникновении сигнала
         для интерфейса impacted-resource может указывать каналы
         агрегированного порта.";
    }
    leaf-list root-cause-resource {
      if-feature "root-cause-analysis";
      type resource;
      description
        "Ресурсы, с которыми может быть связан этот сигнал. Если в
         системе есть механизм определения первопричины сигнала, этот
         leaf-list может служить для перечисления ресурсов, которые
         могут служить первопричиной. За счёт этого система может
         создавать один сигнал вместо нескольких. Примером может
         служить отказ системного журнала, когда сигнал указывает
         файловую систему в root-cause-resource. Отметим, что
         предусмотренное использование не состоит в отправке сигнала
         с указанием root-cause-resource как связанного с тревогой
         ресурса. Лист-список root-cause-resource служит подсказкой
         и не следует создавать сигнал для той же проблемы.";
    }
  }

  grouping alarm-state-change-parameters {
    description
      "Параметры для сены alarm-state. Эта группа применяется в списке
       status-change списка сигналов тревоги и в уведомлениях о смене
       alarm-state.";
    leaf time {
      type yang:date-and-time;
      mandatory true;
      description
        "Время изменения статуса сигнала тревоги. Значение указывает
         фактическое время смены alarm-state в ресурсе, а не момент
         добавления в список аварийных сигналов. Это же значение
         ДОЛЖНО указываться в /alarm-list/alarm/last-changed.";
    }
    leaf perceived-severity {
      type severity-with-clear;
      mandatory true;
      description
        "Важность сигнала в соответствии с X.733. Отметим, что это
         может не быть исходным уровнем, поскольку важность сигнала
         может меняться.";
      reference
        "ITU-T Recommendation X.733: Information Technology
           - Open Systems Interconnection
           - System Management: Alarm Reporting Function";
    }
    leaf alarm-text {
      type alarm-text;
      mandatory true;
      description
        "Текст описания смены alarm-state для пользователя.";
      reference
        "ITU-T Recommendation X.733: Information Technology
           - Open Systems Interconnection
           - System Management: Alarm Reporting Function";
    }
  }

  grouping operator-parameters {
    description
      "Параметры, которые может изменить оператор.";
    leaf time {
      type yang:date-and-time;
      mandatory true;
      description
        "Метка времени для действия оператора по сигналу.";
    }
```

```
      leaf operator {
        type string;
        mandatory true;
        description
          "Имя оператора, действовавшего по сигналу.";
      }
      leaf state {
        type operator-state;
        mandatory true;
        description
          "Представление оператора о статусе сигнала тревоги.";
      }
      leaf text {
        type string;
        description
          "Дополнительные текстовые сведения от оператора.";
      }
    }

    grouping resource-alarm-parameters {
      description
        "Параметры сигнала тревоги с точки зрения ресурса.";
      leaf is-cleared {
        type boolean;
        mandatory true;
        description
          "Указывает текущее состояние очистки сигнала тревоги. Сигнал
           может перейти из active в cleared и наоборот.";
      }
      leaf last-raised {
        type yang:date-and-time;
        mandatory true;
        description
          "Сигнал может менять уровень важности и переключаться между
           active и cleared в течение срока действия. Этот лист
           указывает время последней активации (is-cleared = false).";
      }
      leaf last-changed {
        type yang:date-and-time;
        mandatory true;
        description
          "Метка времени последнего изменения списка status-change или
           operator-state-change.";
      }
      leaf perceived-severity {
        type severity;
        mandatory true;
        description
          "Последний уровень важности аварийного сигнала. Если сигнал
           был подан с уровнем warning, а позднее получил уровень major,
           значением листа будет major.";
      }
      leaf alarm-text {
        type alarm-text;
        mandatory true;
        description
          "Текст последнего сообщённого сигнала, . В этот текст следует
           включать сведения, позволяющие оператору понять и устранить
           problem and how to resolve it.";
      }
      list status-change {
        if-feature "alarm-history";
        key "time";
        min-elements 1;
        description
          "Список событий status-change для этого сигнала тревоги.

           Запись с последней меткой времени в этом списке ДОЛЖНА
           соответствовать листьям is-cleared, perceived-severity,
           alarm-text для сигнала.

           Список упорядочивается по меткам времени смены статуса
           сигнала тревоги, начиная с самой старой метки.

           В список включаются указанные ниже смены состояния
           - смена уровня важности (warning, minor, major, critical)
           - смена статуса очистки (обновляется также is-cleared)
           - обновление alarm-text.";
        uses alarm-state-change-parameters;
      }
    }

    grouping filter-input {
      description
        "Группировка для фильтров сведений о сигналах тревоги.";
      leaf alarm-clearance-status {
```

```
        type enumeration {
          enum any {
            description
              "Игнорировать статус очистки сигнала тревоги.";
          }
          enum cleared {
            description
              "Фильтровать очищенные аварийные сигналы.";
          }
          enum not-cleared {
            description
              "Фильтровать неочищенные аварийные сигналы.";
          }
        }
        mandatory true;
        description
          "Очистка статуса аварийного сигнала.";
      }
      container older-than {
        presence "Указание возраста";
        description
          "Соответствие листу last-changed[1] в аварийном сигнале.";
        choice age-spec {
          description
            "Фильтр по дате и времени (возрасту).";
          case seconds {
            leaf seconds {
              type uint16;
              description
                "Возраст в секундах.";
            }
          }
          case minutes {
            leaf minutes {
              type uint16;
              description
                "Возраст в минутах.";
            }
          }
          case hours {
            leaf hours {
              type uint16;
              description
                "Возраст в часах.";
            }
          }
          case days {
            leaf days {
              type uint16;
              description
                "Возраст в днях.";
            }
          }
          case weeks {
            leaf weeks {
              type uint16;
              description
                "Возраст в неделях.";
            }
          }
        }
      }
      container severity {
        presence "Фильтр важности";
        choice sev-spec {
          description
            "Фильтр по уровню важности.";
          leaf below {
            type severity;
            description
              "Уровень важности меньше этого значения.";
          }
          leaf is {
            type severity;
            description
              "Уровень важности равен этому значению.";
          }
          leaf above {
            type severity;
            description
              "Уровень важности больше этого значения.";
          }
        }
        description
```

[1] В оригинале ошибочно указано last-status-change. См. https://www.rfc-editor.org/errata/eid6866. *Прим. перев.*

```
        "Фильтр на основе уровня важности.";
    }
    container operator-state-filter {
      if-feature "operator-actions";
      presence "Фильтр статуса у оператора";
      leaf state {
        type operator-state;
        description
          "Фильтр по состоянию у оператора.";
      }
      leaf user {
        type string;
        description
          "Фильтр по оператору.";
      }
      description
        "Фильтр по состоянию у оператора.";
    }
  }

  /*
   * Дерево данных /alarms
   */

  container alarms {
    description
      "Контейнер верхнего уровня для модуля.";
    container control {
      description
        "Конфигурация управления поведением сигналов тревоги.";
      leaf max-alarm-status-changes {
        type union {
          type uint16;
          type enumeration {
            enum infinite {
              description
                "Записи status-change собираются бесконечно.";
            }
          }
        }
        default "32";
        description
          "Записи status-change хранятся в кольцевых списках по
           сигналам. Когда число записей превосходит это значение,
           самая старая запись о смене состояния автоматически
           удаляется. Если задано значение infinite, записи
           status-change накапливаются без ограничений.";
      }
      leaf notify-status-changes {
        type enumeration {
          enum all-state-changes {
            description
              "Передавать уведомления для любой смены состояния.";
          }
          enum raise-and-clear {
            description
              "Передавать уведомления только при активации, очистке и
               реактивации. Уведомления о смене уровня важности и
               alarm-text не передаются.";
          }
          enum severity-level {
            description
              "Передавать уведомления только при пересечении
               alarm-state уровня, заданного в notify-severity-level.
               Уведомления об очистке передаются всегда.";
          }
        }
        must '. != "severity-level" or ../notify-severity-level' {
          description
            "При указании severity-level в notify-status-changes
             должно быть задано значение для notify-severity-level.";
        }
        default "all-state-changes";
        description
          "Этот лист управляет передачей уведомлений при обновлении
           статуса сигнала тревоги. Возможны три варианта
           1.  Уведомления передаются для всех обновлений, смены
               уровня важности и alarm-text.
           2.  Уведомления передаются только при активации и очистке
               сигнала.
           3.  Уведомления передаются лишь при достижении и превышении
               заданного уровня важности. Уведомления об очистке
               передаются всегда. Уведомления также передаются, если
               уровень важности становится меньше заданного порога.

           Предположим, например, что для вариант 3 задан уровень
```

```
          major и сигнал меняется, как показано ниже

          [(Time, severity, clear)]:
          [(T1, major, -), (T2, minor, -), (T3, warning, -),
           (T4, minor, -), (T5, major, -), (T6, critical, -),
           (T7, major.  -), (T8, major, clear)]

          Уведомления будут передаваться в моменты
          T1, T2, T5, T6, T7, T8.";
      }
      leaf notify-severity-level {
        when '../notify-status-changes = "severity-level"';
        type severity;
        description
          "Уведомления передаются лишь при пересечении alarm-state
           заданного уровня. Сведения об очистке передаются всегда.";
      }
      container alarm-shelving {
        if-feature "alarm-shelving";
        description
          "Список alarm-shelving/shelf служит для блокировки
           (экранирования) сигналов тревоги. Условия блокировки
           объединяются операцией И (AND). Применяется первая
           соответствующая блокировка и сигналы блокируются лишь для
           неё. Совпадающие сигналы ДОЛЖНЫ появляться в списке
           /alarms/shelved-alarms/shelved-alarm, а несовпадающие
           ДОЛЖНЫ быть в списке /alarms/alarm-list/alarm. Сервер не
           передаёт уведомлений для заблокированных сигналов.

           Сервер ДОЛЖЕН поддерживать статус (например, смену уровня)
           для заблокированных сигналов.

           Сигналам, соответствующим критерию нужно иметь статус
           shelved у оператора. При удалении конфигурации блокировки
           серверу нужно установить у оператора статус un-shelved.";
        list shelf {
          key "name";
          ordered-by user;
          leaf name {
            type string;
            description
              "Произвольное имя для блокировки сигнала тревоги.";
          }
          description
            "Каждая запись задаёт критерий для блокировки сигналов.
             Критерии объединяются операцией И (AND). Если критерии не
             заданы, блокируются все сигналы.";
          leaf-list resource {
            type resource-match;
            description
              "Блокировать сигналы для соответствующих ресурсов.";
          }
          list alarm-type {
            key "alarm-type-id alarm-type-qualifier-match";
            description
              "Любой сигнал, соответствующий комбинации критериев
               alarm-type-id и alarm-type-qualifier-match ДОЛЖЕН
               соответствовать.";
            leaf alarm-type-id {
              type alarm-type-id;
              description
                "Блокировать все сигналы с alarm-type-id совпадающим с
                 этим идентификатором или производным от него.";
            }
            leaf alarm-type-qualifier-match {
              type string;
              description
                "регулярное выражение XML Schema для сопоставления с
                 классификаторам типа сигнала тревоги. Блокируются все
                 сигналы, классификатор которых соответствует.";
              reference
                "XML Schema Part 2: Datatypes Second Edition,
                   World Wide Web Consortium Recommendation
                   REC-xmlschema-2-20041028";
            }
          }
          leaf description {
            type string;
            description
              "Необязательное текстовое описание блокировки, в котором
               следует указывать причины блокировки сигналов.";
          }
        }
      }
    }
    container alarm-inventory {
```

```
      config false;
      description
        "Список alarm-inventory/alarm-type содержит все возможные типы
         аварийных сигналов для системы.

         Если система знает, для каких ресурсов может появляться
         конкретный сигнал тревоги, это также указывается в описи.
         Список также говорит, имеет ли каждый сигнал соответствующее
         состояние очистки. В описи нужно указывать лишь конкретные
         типы аварийных сигналов.

         Опись сигналов ДОЛЖНА обновляться системой при каждом
         возможном появлении нового сигнала. Это может быть при
         установке новых программных модулей или плат. При изменении
         описи передаётся уведомление alarm-inventory-changed.";
      list alarm-type {
        key "alarm-type-id alarm-type-qualifier";
        description
          "Записи списка указывают возможные сигналы тревоги.";
        leaf alarm-type-id {
          type alarm-type-id;
          description
            "Статический идентификатор типа для этого сигнала.";
        }
        leaf alarm-type-qualifier {
          type alarm-type-qualifier;
          description
            "Необязательный динамический идентификатор типа сигнала.";
        }
        leaf-list resource {
          type resource-match;
          description
            "Указывает, к каким ресурсам применим сигнал (опция).";
        }
        leaf will-clear {
          type boolean;
          mandatory true;
          description
            "Этот лист говорит оператору, будет ли очищен сигнал при
             выполнении верных корректирующих действий. Реализациям
             СЛЕДУЕТ стремиться к обнаружению статуса очистки для всех
             типов аварийных сигналов.

             При значении true оператор может наблюдать сигнал, пока
             тот не будет сброшен после корректировочных действий.

             При значении false оператор должен проверить, что сигнал
             больше не активен, с помощью иного механизма. Сигналы
             могут не очищаться из-за отсутствия соответствующего
             инструмента или логического статуса очистки.";
        }
        leaf-list severity-level {
          type severity;
          description
            "Указывает возможные уровни важности для сигнала тревоги.
             Следует отметить, что clear не относится к важности. В
             общем случае уровень важности следует задавать
             инструментально на основе динамического состояния, а не
             указывать статически, чтобы уровень важности динамически
             соответствовал состоянию и контексту. Однако тип сигнала
             должен иметь набор возможных уровней важности, который
             следует указывать здесь.";
        }
        leaf description {
          type string;
          mandatory true;
          description
            "Описание возможного сигнала тревоги, в которое СЛЕДУЕТ
             включать сведения о возможных первопричинах и действиях
             по исправлению.";
        }
      }
    }
    container summary {
      if-feature "alarm-summary";
      config false;
      description
        "Контейнер для сводки по множеству сигналов.";
      list alarm-summary {
        key "severity";
        description
          "Глобальная сводка сигналов тревоги в системе.
           Заблокированные сигналы в сводку не включаются.";
        leaf severity {
          type severity;
          description
```

```
            "Сводка аварийных сигналов с этим уровнем важности.";
        }
        leaf total {
          type yang:gauge32;
          description
            "Общее число сигналов с этим уровнем важности.";
        }
        leaf not-cleared {
          type yang:gauge32;
          description
            "Общее число не очищенных сигналов с этим уровнем.";
        }
        leaf cleared {
          type yang:gauge32;
          description
            "Число очищенных сигналов с этим уровнем важности.";
        }
        leaf cleared-not-closed {
          if-feature "operator-actions";
          type yang:gauge32;
          description
            "Число сигналов с этим уровнем важности, которые очищены,
             но не закрыты.";
        }
        leaf cleared-closed {
          if-feature "operator-actions";
          type yang:gauge32;
          description
            "Число сигналов с этим уровнем важности, которые очищены
             и закрыты.";
        }
        leaf not-cleared-closed {
          if-feature "operator-actions";
          type yang:gauge32;
          description
            "Число сигналов с этим уровнем важности, которые не
             очищены, но закрыты.";
        }
        leaf not-cleared-not-closed {
          if-feature "operator-actions";
          type yang:gauge32;
          description
            "Число сигналов с этим уровнем важности, которые не
             очищены и не закрыты.";
        }
      }
      leaf shelves-active {
        if-feature "alarm-shelving";
        type empty;
        description
          "Подсказка оператору о активной блокировке сигналов тревоги.
           Этот лист ДОЛЖЕН существовать, если
           /alarms/shelved-alarms/number-of-shelved-alarms > 0.";
      }
    }
    container alarm-list {
      config false;
      description
        "Аварийные сигналы в системе.";
      leaf number-of-alarms {
        type yang:gauge32;
        description
          "Общее число аварийных сигналов в системе, т. е. число
           записей в списке сигналов тревоги.";
      }
      leaf last-changed {
        type yang:date-and-time;
        description
          "Метка времени последнего изменения списка сигналов тревоги.
           Это значение может применяться для управления процессом
           ресинхронизации аварийных сигналов.";
      }
      list alarm {
        key "resource alarm-type-id alarm-type-qualifier";
        description
          "Список сигналов тревоги. Каждая записи списка содержит один
           сигнал для данного типа и ресурса. Сигнал может быть
           обновлён базовым ресурсом или пользователем. Ресурс
           поддерживает листья is-cleared, last-change,
           perceived-severity, alarm-text. Оператор может менять
           operator-state и operator-text.

           Запись появляется в списке при первом возникновении сигнала
           этого типа для данного ресурса. При очистке сигнала запись
           из списка не удаляется. Статус очистки представляется
           логическим флагом.
```

```
        Записи для сигналов удаляются путём явной операции очистки
        (purge). Например, можно удалить все очищенные и закрытые
        сигналы у оператора, которые старше 24 часов. Если статус
        связанного с сигналом ресурса изменится после очистки
        (purge), сигнал снова появится в списке.

        Системы могут удалять сигналы тревоги на основе локально
        заданных правил, но это выходит за рамки модуля.";
    uses common-alarm-parameters;
    leaf time-created {
      type yang:date-and-time;
      mandatory true;
      description
        "Метка времени создания записи для сигнала. Дальнейшие
         изменения этого сигнала не меняют значения метки и
         отражаются в листе last-changed.";
    }
    uses resource-alarm-parameters;
    list operator-state-change {
      if-feature "operator-actions";
      key "time";
      description
        "Список, применяемый операторами для указания участия
         человека, связанного с аварийным сигналом. Например,
         оператор может, увидев сигнал, добавить в этот список
         подтверждение.";
      uses operator-parameters;
    }
    action set-operator-state {
      if-feature "operator-actions";
      description
        "Средство для оператора указать степень вмешательства
         человека в сигнал тревоги.";
      input {
        leaf state {
          type writable-operator-state;
          mandatory true;
          description
            "Состояние у этого оператора.";
        }
        leaf text {
          type string;
          description
            "Дополнительная текстовая информация.";
        }
      }
    }
    notification operator-action {
      if-feature "operator-actions";
      description
        "Указывает, что оператор отреагировал на сигнал тревоги.";
      uses operator-parameters;
    }
  }
  action purge-alarms {
    description
      "Запрашивает у сервера удаление из списка сигналов,
       соответствующих заданным критериям. Обычно это служит для
       удаления закрытых сигналов старше заданного времени.

       На выходе возвращается число удалённых сигналов.";
    input {
      uses filter-input;
    }
    output {
      leaf purged-alarms {
        type uint32;
        description
          "Число удалённых сигналов.";
      }
    }
  }
  action compress-alarms {
    if-feature "alarm-history";
    description
      "Запрашивает у сервера сжатие записей в списке сигналов
       путём удаления всех соответствующих сигналов, кроме
       последней записи status-change. Заданные на входе условия
       объединяются операцией И (AND). Если условия не заданы,
       сжимаются все аварийные сигналы.";
    input {
      leaf resource {
        type resource-match;
        description
          "Сжимать сигналы, соответствующие этому ресурсу.";
```

```
        }
        leaf alarm-type-id {
          type leafref {
            path "/alarms/alarm-list/alarm/alarm-type-id";
            require-instance false;
          }
          description
            "Сжимать сигналы с этим alarm-type-id.";
        }
        leaf alarm-type-qualifier {
          type leafref {
            path "/alarms/alarm-list/alarm/alarm-type-qualifier";
            require-instance false;
          }
          description
            "Сжимать сигналы с этим alarm-type-qualifier.";
        }
      }
      output {
        leaf compressed-alarms {
          type uint32;
          description
            "Число сжатых записей сигналов тревоги.";
        }
      }
    }
  }
  container shelved-alarms {
    if-feature "alarm-shelving";
    config false;
    description
      "Заблокированные сигналы. Это сигналы, соответствующие
       критериям из /alarms/control/alarm-shelving. По этому списку
       не передаётся никаких уведомлений. Список включает сигналы,
       сочтённые неважными для оператора. Эти сигналы имеют
       значение operator-state shelved, которое нельзя изменить.";
    leaf number-of-shelved-alarms {
      type yang:gauge32;
      description
        "Общее число текущих заблокированных сигналов тревоги, т. е.
         записей в списке.";
    }
    leaf shelved-alarms-last-changed {
      type yang:date-and-time;
      description
        "Временная метка последнего изменения заблокированного
         сигнала. Значение может применяться менеджером для
         процедуры ресинхронизации.";
    }
    list shelved-alarm {
      key "resource alarm-type-id alarm-type-qualifier";
      description
        "Список заблокированных сигналов. Эти сигналы может
         обновлять лишь базовый ресурс, но не оператор.";
      uses common-alarm-parameters;
      leaf shelf-name {
        type leafref {
          path "/alarms/control/alarm-shelving/shelf/name";
          require-instance false;
        }
        description
          "Время блокировки.";
      }
      uses resource-alarm-parameters;
      list operator-state-change {
        if-feature "operator-actions";
        key "time";
        description
          "Список, применяемый операторами для указания участия
           человека, связанного с аварийным сигналом. Для
           заблокированных сигналов система устанавливает статус
           shelved.";
        uses operator-parameters;
      }
    }
    action purge-shelved-alarms {
      description
        "Запрашивает у сервера удаление заблокированных сигналов,
         соответствующих заданным критериям. Из списка
         заблокированных имеет смысл удалять сигналы, которые совсем
         не имеют смысла.
         На выходе возвращается число удалённых сигналов.";
      input {
        uses filter-input;
      }
      output {
```

```
          leaf purged-alarms {
            type uint32;
            description
              "Число очищенных (purge) сигналов тревоги.";
          }
        }
      }
      action compress-shelved-alarms {
        if-feature "alarm-history";
        description
          "Запрашивает у сервера сжатие записей в shelved-alarm
           путём удаления всех соответствующих сигналов, кроме
           последней записи status-change. Заданные на входе условия
           объединяются операцией И (AND). Если условия не заданы,
           сжимаются все аварийные сигналы в списке.";
        input {
          leaf resource {
            type leafref {
              path "/alarms/shelved-alarms/shelved-alarm/resource";
              require-instance false;
            }
            description
              "Сжимать сигналы от этого ресурса.";
          }
          leaf alarm-type-id {
            type leafref {
              path "/alarms/shelved-alarms/shelved-alarm"
                 + "/alarm-type-id";
              require-instance false;
            }
            description
              "Сжимать сигналы с этим alarm-type-id.";
          }
          leaf alarm-type-qualifier {
            type leafref {
              path "/alarms/shelved-alarms/shelved-alarm"
                 + "/alarm-type-qualifier";
              require-instance false;
            }
            description
              "Сжимать сигналы с этим alarm-type-qualifier.";
          }
        }
        output {
          leaf compressed-alarms {
            type uint32;
            description
              "Число сжатых записей сигналов тревоги.";
          }
        }
      }
    }
    list alarm-profile {
      if-feature "alarm-profile";
      key "alarm-type-id alarm-type-qualifier-match resource";
      ordered-by user;
      description
        "Задаёт дополнительные сведения или конфигурацию для каждого
         типа аварийных сигналов. Этот модуль поддерживает для клиента
         механизм переопределения заданных системой уровень важности
         сигналов. Список alarm-profile полезен также в качестве точек
         дополнения к конкретным типам сигналов.";
      leaf alarm-type-id {
        type alarm-type-id;
        description
          "Идентификатор типа сигнала для сопоставления.";
      }
      leaf alarm-type-qualifier-match {
        type string;
        description
          "Регулярное выражение XML Schema для сопоставления с
           классификатором типа аварийного сигнала.";
        reference
          "XML Schema Part 2: Datatypes Second Edition,
             World Wide Web Consortium Recommendation
             REC-xmlschema-2-20041028";
      }
      leaf resource {
        type resource-match;
        description
          "Задаёт сопоставляемый ресурс.";
      }
      leaf description {
        type string;
        mandatory true;
        description
```

```
            "Описание профиля сигналов тревоги.";
        }
        container alarm-severity-assignment-profile {
          if-feature "severity-assignment";
          description
            "Клиент может переопределить системный уровень важности.";
          reference
            "ITU-T Recommendation M.3100:
               Generic network information model
             ITU-T Recommendation M.3160:
               Generic, protocol-neutral management information model";
          leaf-list severity-level {
            type severity;
            ordered-by user;
            description
              "Задаёт настроенные уровни важности для соответствующего
               сигнала тревоги. Если у сигнала несколько уровней, их
               нужно указывать в порядке роста важности. Функция
               M3100/M3160 ASAP допускает лишь взаимнооднозначное
               соответствие между типом и важностью, но модуль YANG
               поддерживает сигналы с учётом состояния, поэтому нужно
               разрешать несколько уровней важности для сигнала.

               Предположим сигнал о сильной загрузке с двумя порогами
               для системных уровней важности threshold1 = warning
               и threshold2 = minor. Установка в этом leaf-list пары
               (minor, major) будет задавать уровни
               threshold1 = minor и threshold2 = major";
          }
        }
      }
    }

    /*
     * Уведомления
     */

    notification alarm-notification {
      description
        "Служит для информирования о смене статуса сигнала. Одно
         уведомление применяется для вновь возникшего и сброшенного
         сигнала, а также при изменении текста или важности
         имеющегося сигнала.";
      uses common-alarm-parameters;
      uses alarm-state-change-parameters;
    }

    notification alarm-inventory-changed {
      description
        "Служит для информирования об изменении списка возможных
         сигналов тревоги. Это может случиться, например, при установке
         нового программного модуля или платы.";
    }
  }
  <CODE ENDS>
```

7. Модуль сопоставления с X.733

Многие системы аварийных сигналов основаны на стандартах X.733 [X.733] и X.736 [X.736]. Модель ietf-alarms-x733 дополняет опись сигналов тревоги, список сигналов и уведомления о них параметрами X.733 и X.736. Модуль также поддерживает функцию, с помощью которой можно настроить сопоставления типов сигналов тревоги с параметрами X.733 event-type и probable-cause. Это может потребоваться, если принятое в системе по умолчанию сопоставления будет конфликтовать с другими системами управления или будет сочтено некорректным.

Отметим, что термин ресурс (resource) в этом документе соответствует термину ITU managed object (управляемый объект).

Модуль YANG ссылается на [RFC6991], [X.721], [X.733] и [X.736].

```
  <CODE BEGINS> file "ietf-alarms-x733@2019-09-11.yang"
  module ietf-alarms-x733 {
    yang-version 1.1;
    namespace "urn:ietf:params:xml:ns:yang:ietf-alarms-x733";
    prefix x733;

    import ietf-alarms {
      prefix al;
    }
    import ietf-yang-types {
      prefix yang;
      reference
        "RFC 6991: Common YANG Data Types";
    }

    organization
      "IETF CCAMP Working Group";
```

```
  contact
    "WG Web:   <https://trac.ietf.org/trac/ccamp>
     WG List:  <mailto:ccamp@ietf.org>

     Editor:   Stefan Vallin
               <mailto:stefan@wallan.se>

     Editor:   Martin Bjorklund
               <mailto:mbj@tail-f.com>";
  description
    "Этот модуль дополняет ietf-alarms параметрами сигналов X.733 для
     указанных ниже структур, указывая тип и возможную причину X.733.
      1) alarms/alarm-inventory - все возможные типы сигналов тревоги
      2) alarms/alarm-list - каждый сигнал тревоги в системе
      3) alarm-notification - уведомления о смене alarm-state
      4) alarms/shelved-alarms

     Модуль позволяет системам управления аварийными сигналами
     настраивать отображение ключей сигналов ietf-alarms на пары ITU
     (event-type, probable-cause). Отображение не включает значение
     соответствующей проблемы, специфичное для X.733. Рекомендуется
     применять лист alarm-type-qualifier, служащий для этого.

     Модуль использует целые числа и строки текста для возможных
     причин вместо глобально заданного перечисления, чтобы иметь
     возможность контроля конфликтующих определений перечисляемых
     элементов. Одно глобальное определение перечисляемых элементов
     сложно поддерживать.

     Ключевые слова ДОЛЖНО, НЕДОПУСТИМО, ТРЕБУЕТСЯ, НУЖНО, НЕ НУЖНО,
     СЛЕДУЕТ, НЕ СЛЕДУЕТ, РЕКОМЕНДУЕТСЯ, НЕ РЕКОМЕНДУЕТСЯ, МОЖНО,
     НЕОБЯЗАТЕЛЬНО в этом документе трактуются в соответствии с
     BCP 14 (RFC 2119) (RFC 8174) тогда и только тогда, когда они
     указаны заглавными буквами, как показано здесь.

     Авторские права (Copyright (c) 2019) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Эта версия модуля YANG является частью RFC 8632, где правовые
     аспекты приведены более полно.";
  reference
    "ITU-T Recommendation X.733: Information Technology
       - Open Systems Interconnection
       - System Management: Alarm Reporting Function";

  revision 2019-09-11 {
    description
      "Исходный выпуск.";
    reference
      "RFC 8632: A YANG Data Model for Alarm Management";
  }

  /*
   * Свойства (функции)
   */

  feature configure-x733-mapping {
    description
      "Система поддерживает настраиваемое отображение alarm-type
       из ietf-alarms на X733 event-type и probable-cause.";
  }

  /*
   * Определения типов
   */

  typedef event-type {
    type enumeration {
      enum other {
        value 1;
        description
          "Ничего из перечисленного ниже.";
      }
      enum communications-alarm {
        value 2;
        description
          "Сигнал, связанный в основном с процедурами и/или
           процессами, требуемыми для переноса информации от
           одной точки к другой.";
```

```
        }
        enum quality-of-service-alarm {
          value 3;
          description
            "Сигнал, связанный в основном с отказом со снижением
             качества обслуживания.";
        }
        enum processing-error-alarm {
          value 4;
          description
            "Сигнал, связанный в основном с отказом программы или
             обработки.";
        }
        enum equipment-alarm {
          value 5;
          description
            "Сигнал, связанный в основном с отказом оборудования.";
        }
        enum environmental-alarm {
          value 6;
          description
            "Сигнал, связанный в основном с условием, относящимся к
             шасси, где размещено оборудование.";
        }
        enum integrity-violation {
          value 7;
          description
            "Индикация возможного неправомерного изменение, вставки или
             удаления информации.";
        }
        enum operational-violation {
          value 8;
          description
            "Указание невозможности предоставления запрошенной услуги
             из-за недоступности, неисправности или некорректного
             вызова службы.";
        }
        enum physical-violation {
          value 9;
          description
            "Указывает нарушение физического ресурса способом,
             предполагающим атаку.";
        }
        enum security-service-or-mechanism-violation {
          value 10;
          description
            "Указывает обнаружение атаки службой или механизмом
             безопасности.";
        }
        enum time-domain-violation {
          value 11;
          description
            "Событие произошло в неожиданный или запрещённый момент.";
        }
      }
      description
        "Типы событий, заданные в X.733 и X.736.";
      reference
        "ITU-T Recommendation X.733: Information Technology
           - Open Systems Interconnection
           - System Management: Alarm Reporting Function
         ITU-T Recommendation X.736: Information Technology
           - Open Systems Interconnection
           - System Management: Security Alarm Reporting Function";
    }

    typedef trend {
      type enumeration {
        enum less-severe {
          description
            "Имеется хотя бы один остающийся сигнал тревоги с важностью
             выше (более важный), чем текущий аварийный сигнал.";
        }
        enum no-change {
          description
            "Воспринимаемый уровень важности текущего сигнала совпадает
             с высшим (наиболее важным) из остающихся сигналов.";
        }
        enum more-severe {
          description
            "Воспринимаемый уровень важности текущего сигнала выше чем
             указанный в любом из остающихся сигналов тревоги.";
        }
      }
      description
        "Описывает тенденцию уровня важности сигналов связанного с
```

```
        аварией ресурса.";
    reference
      "ITU-T Recommendation X.721: Information Technology
          - Open Systems Interconnection
          - Structure of management information:
            Definition of management information
            Module Attribute-ASN1Module";
  }

  typedef value-type {
    type union {
      type int64;
      type uint64;
      type decimal64 {
        fraction-digits 2;
      }
    }
    description
      "Общий тип объединения, соответствующий выбору ITU
       целого или действительного числа.";
  }

  /*
   * Группировки
   */

  grouping x733-alarm-parameters {
    description
      "Базовые параметры X.733 для аварийных сигналов.";
    leaf event-type {
      type event-type;
      description
        "Тип события X.733/X.736 для этого сигнала.";
    }
    leaf probable-cause {
      type uint32;
      description
        "Возможная причина X.733 для этого сигнала.";
    }
    leaf probable-cause-string {
      type string;
      description
        "Понятная пользователю строка, соответствующая целочисленному
         значению возможной причины. Строке СЛЕДУЕТ соответствовать
         перечислению X.733, например, значение 27 - это
         localNodeTransmissionError.";
    }
    container threshold-information {
      description
        "Этот параметр нужно указывать, когда сигнал тревоги является
         результатом пересечения порога. ";
      leaf triggered-threshold {
        type string;
        description
          "Идентификатор порога, вызвавшего уведомление.";
      }
      leaf observed-value {
        type value-type;
        description
          "Значение датчика или счётчика, перешедшее порог. Это может
           отличаться от порога, если датчик может меняться,
           например, только на дискретное значение.";
      }
      choice threshold-level {
        description
          "В случае датчика уровень порога задаёт пару пороговых
           значений - первое указывает сам порог, второе -
           гистерезис. Для счётчика указывается только пороговое
           значение.";
        case up {
          leaf up-high {
            type value-type;
            description
              "Порог повышения для сигнала тревоги.";
          }
          leaf up-low {
            type value-type;
            description
              "Порог снижения для очистки сигнала тревоги. Это
               является гистерезисом для датчиков.";
          }
        }
        case down {
          leaf down-low {
            type value-type;
            description
```

```
            "Порог снижения для сигнала тревоги.";
        }
        leaf down-high {
          type value-type;
          description
            "Порог повышения для очистки сигнала тревоги. Это
            является гистерезисом для датчиков.";
        }
      }
    }
    leaf arm-time {
      type yang:date-and-time;
      description
        "Для порога датчика это время последнего перехода через
         порог, время после предыдущего пересечения порога, когда
         значение гистерезиса для порога было превышено, разрешая
         генерацию уведомления для нового перехода через порог.
         Для порога счётчика это время последнего перехода через
         порог или время инициализации сбрасываемого счётчика.";
    }
  }
  list monitored-attributes {
    uses attribute;
    key "id";
    description
      "Необязательный параметр, который определяет один или
       несколько атрибутов ресурса и их значения в момент сигнала";
  }
  leaf-list proposed-repair-actions {
    type string;
    description
      "Необязательный параметр, который применяется, если причина
       сигнала известна и система может предложить одно или
       несколько решений (таких, как включение резервного
       оборудования, повтор действия или замена среды).";
  }
  leaf trend-indication {
    type trend;
    description
      "Задаёт текущую тенденцию уровня важности сигналов для
       ресурса. При наличии листа он указывает наличие одного
       или нескольких сигналов (остающиеся сигналы), которые не
       были очищены и относятся к тому же ресурсу, сто и этот
       (текущий) сигнал. Возможные значения включают:
         more-severe - воспринимаемая важность текущего сигнала
           выше, чем у любого из остающихся;
         no-change - воспринимаемая важность текущего сигнала
           совпадает с наивысшей среди остающихся сигналов;
         less-severe - среди остающихся имеется хотя бы один
           сигнал с важностью выше, чем у текущего сигнала.";
  }
  leaf backedup-status {
    type boolean;
    description
      "Необязательный лист, указывающий, резервируется ли ресурс,
       с которым связан сигнал, что позволяет узнать, были ли
       нарушены условия предоставления услуг клиентам. Применение
       этого поля вместе с perceived-severity обеспечивает сведения
       для независимого определения серьёзности сигнала тревоги и
       способности системы в целом продолжать предоставление услуг.
       Если лист имеет значение true, это указывает, что объект,
       создавший сигнал тревоги, резервируется, а значение
       false говорит об отсутствии резервирования.";
  }
  leaf backup-object {
    type al:resource;
    description
      "Этот лист НУЖНО включать при наличии backedup-status true.
       Лист указывает экземпляр управляемого объекта, резервирующий
       управляемый объект, к которому относится уведомление. Лист
       полезен, например, при резервировании объекта иным объектом
       из пула, выделяемым на подмену динамически.";
  }
  list additional-information {
    key "identifier";
    description
      "Позволяет включать в сигнал тревоги дополнительные сведения.
       Это серия структур данных, каждая из которых содержит три
       элемента: идентификатор, индикатор значимости и сведения
       о проблеме.";
    leaf identifier {
      type string;
      description
        "Тип данных в информационном параметре.";
    }
    leaf significant {
```

```
        type boolean;
        description
          "Устанавливается true, если принимающая система должна быть
           способная разобрать информационный параметр события, чтобы
           полностью понять отчёт.";
      }
      leaf information {
        type string;
        description
          "Дополнительные сведения о сигнале тревоги.";
      }
    }
    leaf security-alarm-detector {
      type al:resource;
      description
        "Указывает датчик сигнала тревоги.";
    }
    leaf service-user {
      type al:resource;
      description
        "Указывает пользователя службы, чей запрос вызвал сигнал
         тревоги, связанный с безопасностью.";
    }
    leaf service-provider {
      type al:resource;
      description
        "Указывает предполагаемого поставщика услуги, вызвавшей
         сигнал тревоги, связанный с безопасностью.";
    }
    reference
      "ITU-T Recommendation X.733: Information Technology
         - Open Systems Interconnection
         - System Management: Alarm Reporting Function
       ITU-T Recommendation X.736: Information Technology
         - Open Systems Interconnection
         - System Management: Security Alarm Reporting Function";
  }

  grouping x733-alarm-definition-parameters {
    description
      "Базовые параметры X.733 для определений сигналов тревоги.
       Эта группировка служит для задания атрибутов сигналов,
       которые можно сопоставить с механизмом alarm-type в модуле
       ietf-alarms.";
    leaf event-type {
      type event-type;
      description
        "Тип сигнала тревоги для этого типа события X.733/X.736.";
    }
    leaf probable-cause {
      type uint32;
      description
        "Тип сигнала тревоги имеет возможной эту причину X.733.
         Модуль задаёт возможные причины целыми числами, а не
         перечислением. Это связано с тем, что основным
         применением возможных причин являются управляющие
         приложения, если они основаны на стандарте X.733. Однако в
         большинстве управляющий приложений имеются свои
         перечисления причин и слияние перечислений из разных систем
         может вызывать конфликты. Используя настраиваемые значения
         uint32, система может работать с перечисляемыми значениями
         в управляющих приложениях.";
    }
    leaf probable-cause-string {
      type string;
      description
        "Строка с понятным пользователю указанием возможной причины";
    }
  }

  grouping attribute {
    description
      "Группировка для сопоставления базовой ссылки ITU с атрибутом";
    leaf id {
      type al:resource;
      description
        "Ресурс, представляющий атрибут.";
    }
    leaf value {
      type string;
      description
        "Значение представлено строкой, поскольку оно может быть
         любого типа.";
    }
    reference
      "ITU-T Recommendation X.721: Information Technology
```

```
            - Open Systems Interconnection
            - Structure of management information:
              Definition of management information
         Module Attribute-ASN1Module";
    }

    /*
     * Параметры X.733 для определений сигналов тревоги, сигналов
     * и уведомлений.
     */

    augment "/al:alarms/al:alarm-inventory/al:alarm-type" {
      description
        "Добавляет сведения отображения X.733 в сводку сигналов.";
      uses x733-alarm-definition-parameters;
    }

    /*
     * Добавляет настраиваемое отображение X.733.
     */

    augment "/al:alarms/al:control" {
      description
        "Добавляет возможности отображения X.733.";
      list x733-mapping {
        if-feature "configure-x733-mapping";
        key "alarm-type-id alarm-type-qualifier-match";
        description
          "Список, позволяющий приложению управления контролировать
           отображения X.733 лоя всех сигналов тревоги в системе. Любая
           запись списка позволяет менеджеру сигналов тревоги
           переопределить отображение X.733 и в описи сигналов будет
           указано финальное сопоставление.";
        leaf alarm-type-id {
          type al:alarm-type-id;
          description
            "Сопоставление типа сигнала с идентификатором типа.";
        }
        leaf alarm-type-qualifier-match {
          type string;
          description
            "регулярное выражение W3C, применяемое при сопоставлении
             типа и классификатора сигнала с параметрами X.733.";
        }
        uses x733-alarm-definition-parameters;
      }
    }

    augment "/al:alarms/al:alarm-list/al:alarm" {
      description
        "Добавление информации X.733 для сигнала.";
      uses x733-alarm-parameters;
    }

    augment "/al:alarms/al:shelved-alarms/al:shelved-alarm" {
      description
        "Добавление информации X.733 для сигнала.";
      uses x733-alarm-parameters;
    }

    augment "/al:alarm-notification" {
      description
        "Добавление информации X.733 для уведомления о сигнале.";
      uses x733-alarm-parameters;
    }
  }
  <CODE ENDS>
```

8. Взаимодействие с IANA

Этот документ регистрирует два URIs в реестре IETF XML Registry в соответствии с [RFC3688].

```
      URI: urn:ietf:params:xml:ns:yang:ietf-alarms
      Registrant Contact: The IESG.
      XML: N/A; запрошенный URI является пространством имён XML.

      URI: urn:ietf:params:xml:ns:yang:ietf-alarms-x733
      Registrant Contact: The IESG.
      XML: запрошенный URI является пространством имён XML.
```

Документ регистрирует два модуля YANG в реестре YANG Module Names [RFC6020].

```
      name:         ietf-alarms
      namespace:    urn:ietf:params:xml:ns:yang:ietf-alarms
      prefix:       al
      reference:    RFC 8632

      name:         ietf-alarms-x733
```

```
namespace:   urn:ietf:params:xml:ns:yang:ietf-alarms-x733
prefix:      x733
reference:   RFC 8632
```

9. Вопросы безопасности

Заданные в этом документе модули YANG определяют схему для данных, которые предназначены для доступа через сеть с помощью протоколов управления, таких как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый сетевой транспорт с обязательной реализацией протокола SSH[1] [RFC6242], а нижним уровнем RESTCONF - протокол HTTPS с обязательной реализацией TLS [RFC5246].

Модель контроля доступа NETCONF (Network Configuration Access Control Model или NACM) [RFC8341] позволяет разрешать доступ к заданному подмножеству доступных операций и содержимого NETCONF или RESTCONF лишь уполномоченным пользователям NETCONF или RESTCONF.

Список сигналов тревоги сам может чувствительным в плане безопасности, поскольку он может дать атакующему достоверную картину (нарушенного) состояния сети.

В этих модулях данных YANG имеется множество узлов, для которых возможна запись, создание и/или удаление (значение config true, которое устанавливается по умолчанию). Такие узлы могут считаться деликатными или уязвимыми в некоторых сетевых средах. Операции записи (например, edit-config) в такие узлы без подобающей защиты могут оказать негативное влияние на работу сети. Ниже перечислены узлы и ветви модуля ietf-alarms, которые могут быть уязвимы.

/alarms/control/notify-status-changes
: Этот лист указывает, следует ли сигналу тревоги уведомлять о смене состояний системы. Несанкционированный доступ к листу может негативно влиять на рабочие процедуры, основанный на точных отчётах об изменении статуса сигналов тревоги.

/alarms/control/alarm-shelving/shelf
: Этот список управляет блокировкой аварийных сигналов. Несанкционированный доступ может нарушить работу процедур управления сигналами тревоги.

/alarms/control/alarm-profile/alarm-severity-assignment-profile
: Этот список управляет важностью сигналов тревоги. Несанкционированный доступ может позволить, например, снизить уровень важности сигнала, что может негативно повлиять на процессы слежения за сигналами.

Некоторые из операций RPC в этом модуле YANG могут быть чувствительны или уязвимы в той или иной сетевой среде. Важно контролировать доступ к таким операциям. Ниже указаны такие операции.

/alarms/alarm-list/purge-alarms
: Это действие удаляет сигналы тревоги из списка. Несанкционированное применение действия может нарушить работу процедур управления сигналами, поскольку удалённый сигнал может быть важен для работы системы управления аварийными сигналами.

/alarms/alarm-list/alarm/set-operator-state
: Это действие оператор может использовать для указания степени вмешательства человека по сигналу тревоги. Несанкционированное применение действия может приводить к игнорированию сигналов операторами.

10. Литература

10.1. Нормативные документы

[M.3100] International Telecommunication Union, "Generic network information model", ITU-T Recommendation M.3100, April 2005, <https://www.itu.int/rec/T-REC-M.3100-200504-I/en>.

[M.3160] International Telecommunication Union, "Generic, protocol-neutral management information model", ITU-T Recommendation M.3100, November 2008, <https://www.itu.int/rec/T-REC-M.3160-200811-I>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[1]Secure Shell - защищённая оболочка.

[RFC8348] Bierman, A., Bjorklund, M., Dong, J., and D. Romascanu, "A YANG Data Model for Hardware Management", RFC 8348, DOI 10.17487/RFC8348, March 2018, <https://www.rfc-editor.org/info/rfc8348>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[X.721] International Telecommunication Union, "Information technology - Open Systems Interconnection - Structure of management information: Definition of management information", ITU-T Recommendation X.721, February 1992, <https://www.itu.int/rec/T-REC-X.721-199202-I/en>.

[X.733] International Telecommunication Union, "Information technology - Open Systems Interconnection — Systems Management: Alarm reporting function", ITU-T Recommendation X.733, February 1992, <https://www.itu.int/rec/T-REC-X.733-199202-I/en>.

[XSD-TYPES] Malhotra, A. and P. Biron, "XML Schema Part 2: Datatypes Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-2-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028>.

10.2. Дополнительная литература

[ALARMIRP] 3GPP, "Telecommunication management; Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS)", 3GPP TS 32.111-2, March 2005, <http://www.3gpp.org/ftp/Specs/html-info/32111-2.htm>.

[ALARMSEM] Wallin, S., Leijon, V., Nordlander, J., and N. Bystedt, "The semantics of alarm definitions: enabling systematic reasoning about alarms", International Journal of Network Management, Volume 22, Issue 3, May 2012, <http://dx.doi.org/10.1002/nem.800>.

[EEMUA] "Alarm systems: a guide to design, management and procurement", EEMUA Publication No. 191, Engineering Equipment and Materials Users Association, Second Edition, 2007.

[G.7710] International Telecommunication Union, "SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS - Data over Transport - Generic aspects - Transport network control aspects; Common equipment management function requirements", ITU-T Recommendation G.7710/Y.1701, Amendment 1, November 2012.

[ISA182] International Society of Automation, "Management of Alarm Systems for the Process Industries", ANSI/ISA - 18.2-2016, March 2016.

[RFC3877] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, DOI 10.17487/RFC3877, September 2004, <https://www.rfc-editor.org/info/rfc3877>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[X.736] International Telecommunication Union, "Information technology - Open Systems Interconnection - Systems Management: Security alarm reporting function", ITU-T Recommendation X.736, January 1992, <https://www.itu.int/rec/T-REC-X.736-199201-I/en>.

[YANG-INSTANCE] Lengyel, B. and B. Claise, "YANG Instance Data File Format", Work in Progress[1], draft-ietf-netmod-yang-instance-file-format-02, August 2019.

Приложение A. Примеры фирменных типов сигналов

В примере показано, как определить сигналы тревоги в фирменном модуле производителя. Здесь производитель xyz задаёт идентификаторы верхнего уровня по типам событий X.733.

```
module example-xyz-alarms {
  namespace "urn:example:xyz-alarms";
  prefix xyz-al;

  import ietf-alarms {
    prefix al;
  }

  identity xyz-alarms {
    base al:alarm-type-id;
  }

  identity communications-alarm {
    base xyz-alarms;
  }
  identity quality-of-service-alarm {
    base xyz-alarms;
  }
  identity processing-error-alarm {
    base xyz-alarms;
  }
  identity equipment-alarm {
    base xyz-alarms;
  }
  identity environmental-alarm {
    base xyz-alarms;
  }
```

[1]Опубликовано в RFC 9195. *Прим. перев.*

```
  // Коммуникационные сигналы тревоги
  identity link-alarm {
    base communications-alarm;
  }

  // Сигналы QoS
  identity high-jitter-alarm {
    base quality-of-service-alarm;
  }
}
```

Приложение B. Пример сводки аварийных сигналов

Здесь показана опись аварийных сигналов. Один тип сигналов определён только идентификатором, другой настраивается динамически. В последнем случае цифровой вход подключён к датчику дыма, поэтому для alarm-type-qualifier выбран классификатор smoke-detector, а для alarm-type-id - environmental-alarm.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
        xmlns:xyz-al="urn:example:xyz-alarms"
        xmlns:dev="urn:example:device">
  <alarm-inventory>
    <alarm-type>
      <alarm-type-id>xyz-al:link-alarm</alarm-type-id>
      <alarm-type-qualifier/>
      <resource>
        /dev:interfaces/dev:interface
      </resource>
      <will-clear>true</will-clear>
      <description>
        Отказ канала, рабочее состояние down, административное - up.
      </description>
    </alarm-type>
    <alarm-type>
      <alarm-type-id>xyz-al:environmental-alarm</alarm-type-id>
      <alarm-type-qualifier>smoke-alarm</alarm-type-qualifier>
      <will-clear>true</will-clear>
      <description>
        Датчик дыма подключён к цифровому входу.
      </description>
    </alarm-type>
  </alarm-inventory>
</alarms>
```

Приложение C. Пример списка сигналов тревоги

В этом примере показаны смена состояния сигнала тревоги [major, clear, major]. Оператор подтвердил сигнал.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
        xmlns:xyz-al="urn:example:xyz-alarms"
        xmlns:dev="urn:example:device">
  <alarm-list>
    <number-of-alarms>1</number-of-alarms>
    <last-changed>2018-04-08T08:39:50.00Z</last-changed>
    <alarm>
      <resource>
        /dev:interfaces/dev:interface[name='FastEthernet1/0']
      </resource>
      <alarm-type-id>xyz-al:link-alarm</alarm-type-id>
      <alarm-type-qualifier></alarm-type-qualifier>
      <time-created>2018-04-08T08:20:10.00Z</time-created>
      <is-cleared>false</is-cleared>
      <alt-resource>1.3.6.1.2.1.2.2.1.1.17</alt-resource>
      <last-raised>2018-04-08T08:39:40.00Z</last-raised>
      <last-changed>2018-04-08T08:39:50.00Z</last-changed>
      <perceived-severity>major</perceived-severity>
      <alarm-text>
        Рабочее состояние канала down, административное - up.
      </alarm-text>
      <status-change>
        <time>2018-04-08T08:39:40.00Z</time>
        <perceived-severity>major</perceived-severity>
        <alarm-text>
          Рабочее состояние канала down, административное - up.
        </alarm-text>
      </status-change>
      <status-change>
        <time>2018-04-08T08:30:00.00Z</time>
        <perceived-severity>cleared</perceived-severity>
        <alarm-text>
          Рабочее состояние канала up, административное - up.
        </alarm-text>
      </status-change>
      <status-change>
        <time>2018-04-08T08:20:10.00Z</time>
        <perceived-severity>major</perceived-severity>
        <alarm-text>
```

```
            Рабочее состояние канала up, административное - up.
          </alarm-text>
        </status-change>
        <operator-state-change>
          <time>2018-04-08T08:39:50.00Z</time>
          <state>ack</state>
          <operator>joe</operator>
          <text>Будет изучаться, квитанция TR764999</text>
        </operator-state-change>
      </alarm>
    </alarm-list>
  </alarms>
```

Приложение D. Пример блокировки аварийных сигналов

В примере показано, как блокировать сигналы тревоги. Здесь блокируются сигналы, связанные с детекторами дыма, поскольку они недавно установлены и тестируются. Заблокированы также все сигналы от интерфейса FastEthernet1/0.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
        xmlns:xyz-al="urn:example:xyz-alarms"
        xmlns:dev="urn:example:device">
  <control>
    <alarm-shelving>
      <shelf>
        <name>FE10</name>
        <resource>
          /dev:interfaces/dev:interface[name='FastEthernet1/0']
        </resource>
      </shelf>
      <shelf>
        <name>detectortest</name>
        <alarm-type>
          <alarm-type-id>
            xyz-al:environmental-alarm
          </alarm-type-id>
          <alarm-type-qualifier-match>
            smoke-alarm
          </alarm-type-qualifier-match>
        </alarm-type>
      </shelf>
    </alarm-shelving>
  </control>
</alarms>
```

Приложение E. Пример отображения X.733

В примере показано, как сопоставить сигнал тревоги динамического типа (alarm-type-id=environmental-alarm, alarm-type-qualifier=smoke-alarm) с соответствующими параметрами X.733 event-type и probable-cause.

```
<alarms xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms"
        xmlns:xyz-al="urn:example:xyz-alarms">
  <control>
    <x733-mapping
       xmlns="urn:ietf:params:xml:ns:yang:ietf-alarms-x733">
      <alarm-type-id>xyz-al:environmental-alarm</alarm-type-id>
      <alarm-type-qualifier-match>
        smoke-alarm
      </alarm-type-qualifier-match>
      <event-type>quality-of-service-alarm</event-type>
      <probable-cause>777</probable-cause>
    </x733-mapping>
  </control>
</alarms>
```

Приложение F. Связь с другими стандартами

В этом приложении кратко рассмотрена связь модели данных для сигналов тревоги с другими стандартами.

F.1. Определение сигналов тревоги

В таблице 1 приведены определения термина alarm (сигнал тревоги, аварийный сигнал) в других стандартах.

Таблица 1. Определения термина Alarm в стандартах.

Стандарт	*Определение*	*Комментарии*
X.733 [X.733]	Ошибка. Отклонение системы от нормальной работы. Отказ. Физическая или алгоритмическая причина неисправности, проявляющейся как ошибка. Сигнал тревоги. Уведомление в определённой этой функцией форме о конкретном событии. Сигнал тревоги не всегда представляет ошибку.	Определение сигнала тревоги в X.733 сосредоточено на уведомлении, а не на состоянии. X.733 определяет сигнал тревоги как отклонение от нормальных условий, не обязательно требующее корректировочных действий.
G.7710 [G.7710]	Сигналы тревоги - это индикация, автоматически подаваемая устройством при обнаружении отказа.	Определение G.7710 близко к исходному определению X.733.

Alarm MIB [RFC3877]	Сигнал тревоги - это сохраняющаяся индикация отказа. Ошибка - отклонение системы от нормальной работы.	В RFC 3877 сигнал тревоги определён как отклонение от нормальной работы. Модель данных YANG для сигналов тревоги добавляет требование корректировочных действий, что говорит о нежелательности, а не только об отклонении от нормальной работы. База MIB для сигналов тревоги похожа в этом смысле на модуль YANG и сосредоточена на длительном состоянии, а не на отдельных уведомлениях.
ISA [ISA182]	Сигнал тревоги - звуковая и/или визуальная индикация для оператора неисправности оборудования, отклонения процесса или аномальных условий, где требуется реагирование.	Стандарт ISA добавляет важное требование отклонения от нормального состояния, требующего реагирования.
EEMUA [EEMUA]	Сигнал тревоги - это событие, на которое оператор должен осознанно реагировать, отвечать и подтверждать (а не просто подтвердить и забыть).	Это основа определения сигнала тревоги в данном документе. Основное внимание уделено необходимости реального действия.
3GPP Alarm IRP [ALARMIRP]	3GPP v15 называет сигналом тревоги указание нежелательных условий для ресурса (например, канала, устройства), требующее действиия оператора. Подчёркивается ключевое требование, что оператора [...] не следует информировать о нежелательных условиях, пока они не требуют действий. 3GPP v12 считает аварийным сигналом аномальное состояние объекта сети, которое классифицирует событие как отказ. Отказом считается отклонение системы от нормальной работы, которое может приводить к потере операционных возможностей [...]	Последняя версия 3GPP Alarm IRP использует точно такое же определение сигнала тревоги, как и эта модель данных. Следует отметить, что в ранних версиях использовалось определение, не требующее действий оператора, и более широкое определение отклонения от нормальных условий. Ранняя версия также определяла сигнал тревоги как особый случай события.

В процессе эволюции определения сигнала тревоги произошло смещение акцента от событий, оповещающих об отклонении от нормальных условий работы, к нежелательному состоянию, требующему действий оператора.

F.2. Модель данных

Здесь описано, как модель данных YANG для сигналов тревоги связана с моделями из других стандартов. Отметим, что рассматриваются модели данных для интерфейсов аварийных сигналов, а не другие стандарты, такие как специфичные для SDO аварийные сигналы.

F.2.1. X.733

X.733 служит базой для нескольких моделей данных сигналов тревоги в течение лет. Отличия от модели данных YANG перечислены ниже.

X.733 представляет список аварийных сигналов как список уведомлений. Модель данных YANG определяет список сигналов тревоги как список текущих состояний сигналов, который создаётся по уведомлениям о смене статуса.

В X.733 для сигналов тревоги имеется уровень clear (очищен). В модели YANG clear не является уровнем важности, это отдельное состояние аварийного сигнала. Сигнал тревоги может иметь, например, состояния (major, cleared) и (minor, not cleared).

X.733 использует плоский глобально заданный список перечисляемых probable-cause для указания типа сигналов тревоги. Описанная здесь модель использует иерархическое отождествления YANG alarm-type. Это позволяет организациям определять свои типы аварийных сигналов, а также применять абстрактные типы сигналов тревоги, соответствующие базовым идентификаторам (3.2. Тип сигнала тревоги).

Модель данных YANG для сигналов тревоги не включает большинство атрибутов аварийных сигналов X.733, вместо этого они определяются в модуле дополнения [X.733], если требуется строгое соответствие X.733.

F.2.2. Alarm MIB (RFC 3877)

MIB в RFC 3877 использует другой подход - вместо задания конкретной модели данных для сигналов тревоги определена модель сопоставления имеющихся объектов, управляемых по SNMP, и уведомлений с состояниями сигналов тревоги и уведомлениями о сигналах. Это было необходимо, поскольку базы MIB уже были определены для управляемых объектов и уведомлений, указывающих сигналы тревоги, например, уведомления linkUp и linkDown в сочетании с ifAdminState и ifOperState. Поэтому RFC 3877 реально не сравнивается с модулем YANG в этом смысле.

Alarm MIB сопоставляет имеющиеся определения MIB с сигналами тревоги, такими как alarmModelTable. Преимущество этого состоит в том, что менеджер SNMP может в процессе работы считывать возможные типы сигналов тревоги. Это соответствует alarmInventory в модуле YANG.

F.2.3. 3GPP Alarm IRP

3GPP Alarm IRP является развитием X.733. Основные различия между модулем YANG и 3GPP указаны ниже.

3GPP сохраняет большинство атрибутов X.733, модуль YANG - нет.

В 3GPP введены перекрывающиеся и, возможно, конфликтующие ключи для сигналов тревоги alarmId и квартет (managed object, event type, probable cause, specific problem), см. пример 3 в Annex C [ALARMIRP]. В модели данных YANG ключ для идентификации экземпляра аварийного сигнала чётко определён тройкой (resource, alarm-type-id, alarm-type-qualifier), см. 3.4. Идентификация экземпляров аварийных сигналов.

Модуль YANG для сигналов тревоги чётко разделяет жизненный цикл сигнала в ресурсе (измерителе) и у оператора. 3GPP разрешает операторам устанавливать для уровня важности значение clear, что не разрешено в описанном здесь модуле. Вместо этого оператор закрывает сигнал, что не влияет на уровень важности.

F.2.4. G.7710

G.7710 отличается от упомянутых выше стандартов для аварийных сигналов, он не задаёт модели данных для информирования о сигналах тревоги. Стандарт определяет общие требования к функциям управления оборудованием и предназначен для транспортных сетей.

Требования G.7710 соответствуют функциям (feature) модуля YANG, как указано ниже.

Alarm Severity Assignment Profile (ASAP)
Профиль /alarms/alarm-profile/.

Alarm Reporting Control (ARC)
Блокировка сигналов /alarms/control/alarm-shelving/ и возможность контролировать уведомления о сигналах /alarms/control/notify-status-changes. Блокировка сигналов соответствует варианту отключения отчётов о сигналах тревоги для конкретного ресурса - состояние NALM (No ALarM) в M.3100.

Приложение G. Требования к применимости аварийных сигналов

В этом приложении рассмотрены требования к применимости сигналов тревоги, которые важны для интерфейса аварийных сигналов. Модель данных поможет при определении формата, но если фактические сигналы тревоги малозначимы, цель управления аварийными сигналами не будет достигнута.

Основные проблемы, связанные с аварийными сигналами, и их причины указаны в таблице 2. Эта сводка адаптирована для работы в сетях на основе стандартов ISA [ISA182] и EEMUA (Engineering Equipment Materials Users Association) [EEMUA].

Таблица 2. Проблемы и причины аварийных сигналов.

Проблема	***Причина***	***Решение проблемы***
Сигналы генерируются, но оператор игнорирует их.	Раздражающие сигналы (дребезжащие и мимолётные), неисправное оборудование, избыточные сигналы, некорректные настройки сигналов, нерационализированные сигналы, сигналы, представляющие скорей записи системного журнала, чем фактические аварии.	Строгое определение аварийных сигналов, требующих корректировочных действий. См. таблицу 3.
При наличии сигнала оператор не знает, как действовать.	Нечёткие процедуры реагирования на сигналы и нечётко определённые типы аварийных сигналов.	Опись аварийных сигналов со всеми типами сигналов и корректировочными действиями. См. таблицу 3.
Сигналов выдаётся слишком много даже при отсутствии реальных проблем.	Раздражающие сигналы, устаревшие сигналы и сигналы от оборудования, которое не эксплуатируется.	Определения и блокировка аварийных сигналов.
При возникновении отказа оператор получает очень много сигналов и не знает, какие из них важнее.	Некорректная приоритизация сигналов, отказ от использования расширенных методов (например, сигналов на основе состояний).	Модель основанных на состояниях аварийных сигналов и требования к частоте сигналов. См. таблицы 4 и 5.

С учётом этих проблем в EEMUA даны приведённые ниже определения «хороших» сигналов тревоги.

Таблица 3. Определение «хороших» сигналов.

Характеристика	***Объяснение***
Соответствие (релевантность)	Сигналы не являются ложными и малозначительными.
Уникальность	Сигналы не дублируют друг друга.
Своевременность	Не слишком поздно, чтобы можно было ещё что-то сделать.
Приоритизация	Указывается важность проблемы, с которой имеет дело оператор.
Понятность	Сообщение является чётким и простым для понимания.
Диагностика	Указывается проблема, которая возникла.
Консультативность	Указываются действия, которые нужно предпринять.
Сфокусированность	Привлекается внимание к наиболее важным вопросам.

Производителям **следует** рационализировать все сигналы тревоги в соответствии с таблицей 3. Другим важным требованием является частота уведомлений о сигналах тревоги. Производителям **следует** убедиться, что частота не превышает рекомендации EEMUA в таблице 4.

Таблица 4. Допустимая частота передачи аварийных сигналов в установившемся состоянии.

Долгосрочная частота сигналов в стабильном состоянии	***Приемлемость***
Более 1 в минуту	Скорей всего неприемлемо
Одно за 2 минуты	Скорей всего избыточно
Одно за 5 минут	Допустимо
Меньше одного за 10 минут	Скорей всего приемлемо

Таблица 5. Допустимые скорости аварийных сигналов в пиках.

Число аварийных сигналов, отображаемых за 10 минут после важной сетевой проблемы	***Приемлемость***
Более 100	Чрезмерно и скорей всего приведёт к отказу оператора от использования системы аварийной сигнализации.
20-100	Тяжело справиться.
Менее 10	Допустимо, но могут возникать сложности, если несколько сигналов тревоги требуют сложных действий оператора.

Значения в таблицах 4 и 5 указаны для суммы всех аварийных сигналов для сети, контролируемых с одной консоли. Таким образом, каждая отдельная система и NMS (Network Management System) вносит свой вклад.

Производителям **следует** при разработке интерфейса аварийных сигналов обеспечивать выполнение приведённых ниже правил.

1. Рационализация сигналов тревоги в системе, чтобы каждый сигнал был необходимым, имел своё назначение и соответствовал основному правилу, требующему реакции оператора (Таблица 3).
2. Проверка качества аварийных сигналов. Следует обсудить с операторами фактическую полезность сигналов тревоги. Знают ли они, что делать при сигнале? Способны ли быстро найти проблему и выполнить требуемые действия? Соответствует ли текст аварийного сигнала требованиям таблицы 3?
3. Анализ и оценка производительности системы, а также сравнение с параметрами из таблиц 4 и 5. Начать следует с определения мешающих сигналов, а также сохраняющихся сигналов в нормальном состоянии и при запуске.

Благодарности

Авторы благодарны Viktor Leijon и Johan Nordlander за ценный вклад в модель сигналов тревоги.

Спасибо Nick Hancock, Joey Boyd, Tom Petch, Balazs Lengyel за рецензии и вклад в документ.

Адреса авторов

Stefan Vallin
Stefan Vallin AB
Email: stefan@wallan.se

Martin Bjorklund
Cisco
Email: mbj@tail-f.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru