Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1542

(09/2016)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Обмен информацией о кибербезопасности – Обмен информацией о событии/инциденте/эвристических правилах

Формат обмена информационными сообщениями сеанса

Рекомендация МСЭ-Т X.1542

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	**X.1540–X.1549**
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Рекомендация МСЭ-Т X.1542

Формат обмена информационными сообщениями сеанса

Резюме

В современной сетевой среде компьютерные сети уязвимы перед внутренними и внешними угрозами организации. Системы сетевой защиты регистрируют информацию о сеансе, которая касается отдельных входящих и исходящих соединений по протоколу управления передачей/протоколу Интернет (TCP/IP).

Однако эти имеющиеся в настоящее время системы, как правило, функционально несовместимы, потому что каждая система обладает собственными специальными функциональными возможностями, механизмами управления и форматами журнала регистрации сеансов. Сегодня большинство администраторов систем безопасности сталкиваются с необходимостью обеспечения согласованного формата обмена информацией о сеансе для разных систем сетевой защиты и даже разных инфраструктур.

В Рекомендации МСЭ-Т X.1542 приводится информационная модель для формата обмена информационными сообщениями о сеансе (SIMEF), а также относящаяся к ней модель данных, определяемая с помощью схемы расширяемого языка разметки (XML). В SIMEF определяется представление модели данных для обмена информацией транспортного уровня, содержащейся в журнале регистрации сеансов, которая касается централизованного управления безопасностью сети и системы обмена информацией о безопасности. Спецификация какого-либо транспортного протокола не входит в сферу применения настоящей Рекомендации.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1542	07.09.2016 г.	17-я	11.1002/1000/12852

Ключевые слова

Модель данных, обмен сообщениями, безопасность сети, информация о сеансе.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

			Стр.
1	Сфера применения		1
2	Справочные материалы		1
3	Определения		1
	3.1	Термины, определенные в других документах	1
	3.2	Термины, определенные в настоящей Рекомендации	1
4	Сокращения и акронимы		1
5	Условные обозначения		2
6	Обзор		2
7	Представление и определение информации		3
	7.1	XML-документ SIMEF	3
	7.2	Типы данных SIMEF	3
8	Модель данных SIMEF		5
	8.1	Общие сведения о модели данных	6
	8.2	Классы сообщений	7
9	Соображения по вопросам безопасности		26
Дополнение I – Пример и схема SIMEF			27
	I.1	Схема SIMEF	27
	I.2	Примеры SIMEF	28
Библиография			31

Рекомендация МСЭ-Т X.1542

Формат обмена информационными сообщениями сеанса

1 Сфера применения

Настоящая Рекомендация содержит описание формата обмена информационными сообщениями сеанса (SIMEF) и модели данных для представления информации о сеансе, экспортируемой системами безопасности, такими как брандмауэры, а также обоснование использования этой модели. Представлена реализация модели данных на расширяемом языке разметки (XML), разработано определение типа документа (DTD) на языке XML и приведены примеры.

2 Справочные материалы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации содержится определение следующих терминов:

3.2.1 анализатор (analyzer): Система обеспечения безопасности сети, которая обнаруживает атаки путем анализа входящей и исходящей информации о сеансе. Она также создает журнал сеанса и передает его системам управления безопасностью.

3.2.2 информация о сеансе (session information): Информация включает сеанс протокола управления передачей/протокола датаграмм пользователя (TCP/UDP), прикладные услуги и участников сеанса с точки зрения поставщиков информации о сеансе. Сеанс определяется как совокупность видов трафика, которая для целей управления рассматривается как элемент, подлежащий трансляции. Сеансы TCP/UDP однозначно определяются набором данных (исходный IP-адрес, TCP/UDP-порт источника, конечный IP-адрес, TCP/UDP-порт назначения).

ПРИМЕЧАНИЕ. – Определение основано на [b-IETF RFC 2663].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

BSD	Berkeley Software Distribution		Система распространения программного обеспечения Беркли
CGI	Common Gateway Interface		Общий интерфейс шлюзов
DTD	Document Type Definition		Определение типа документа
FTP	File Transfer Protocol		Протокол передачи файлов
HTTP	HyperText Transfer Protocol		Протокол передачи гипертекста
IP	Internet Protocol		Протокол Интернет
LAN	Local Area Network	ЛВС	Локальная вычислительная сеть
MAC	Media Access Control		Управление доступом к среде передачи
NAT	Network Address Translation		Трансляция сетевых адресов
NTP	Network Time Protocol		Сетевой протокол синхронизации времени

POSIX	Portable Operating System Interface	Интерфейс переносимой операционной системы
SIMEF	Session Information Message Exchange Format	Формат обмена информационными сообщениями о сеансе
SNA	Shared Network Architecture	Совместно используемая сетевая архитектура
SNMP	Simple Network Management Protocol	Простой протокол управления сетью
TCP	Transmission Control Protocol	Протокол управления передачей
UDP	User Datagram Protocol	Протокол датаграмм пользователя
UML	Unified Modelling Language	Унифицированный язык моделирования
URL	Uniform Resource Locator	Унифицированный указатель ресурса
UTF	Universal character set Transformation Format	Формат преобразования универсального набора символов
VPN	Virtual Private Network	Виртуальная частная сеть
XML	extensible Markup Language	Расширяемый язык разметки

5 Условные обозначения

UNIX ® – зарегистрированный товарный знак Открытой группы (Open Group).

POSIX ® – зарегистрированный товарный знак IEEE.

6 Обзор

В современной сетевой среде компьютерные сети уязвимы перед внутренними и внешними угрозами организации. Поэтому большинство исследований в области безопасности сетей посвящено разработке комплексных систем управления безопасностью сети и средств мониторинга сети, которые позволяют организации перехватывать пакеты TCP/IP, проходящие через ее сетевые устройства, и рассматривать собранные данные как последовательности диалогов между клиентами и серверами. Например, системы брандмауэров регистрируют информацию о сеансах выбранных входящих и исходящих TCP/IP-соединений.

Концепция SIMEF показана на рисунке 1. Информацию о сеансе можно собрать из систем брандмауэров, устройств трансляции сетевых адресов (NAT) и т. д. SIMEF описывает модель данных, которая охватывает сетевые соединения клиент/сервер, устройство конечного пользователя и прикладные услуги. SIMEF определяет модель данных и соответствующие классы сообщений для передачи надлежащей информации о сеансе транспортного уровня в системы управления безопасностью и системы обмена информацией. Она может применяться системой обмена информацией о проникновениях.

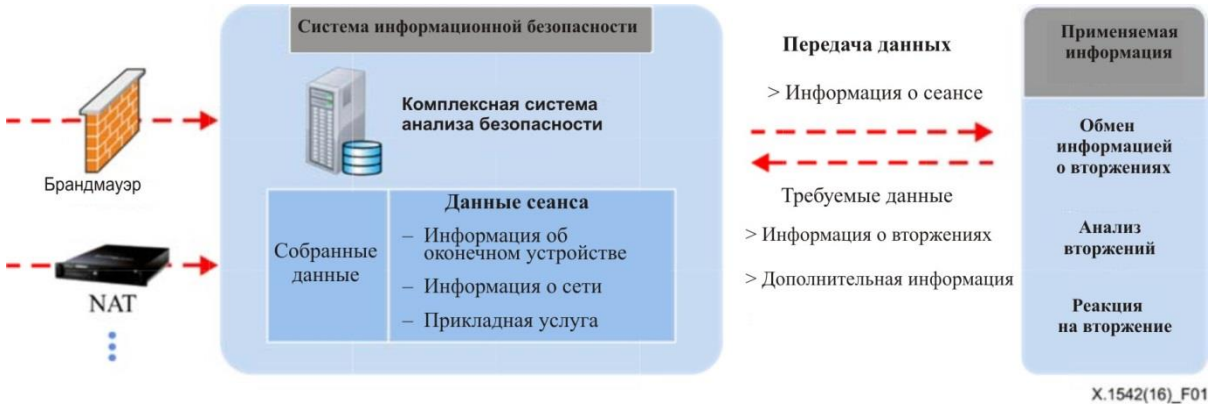

Рисунок 1 – Концепция SIMEF

7 Представление и определение информации

В настоящей Рекомендации используются три системы представления информации: унифицированный язык моделирования (UML) для описания модели данных, XML для описания разметки, используемой в документах SIMEF, и разметка SIMEF для представления самих документов.

7.1 XML-документ SIMEF

В этом пункте описываются правила форматирования XML-документа SIMEF. Большинство этих правил "унаследованы" из правил форматирования XML-документов. В пунктах 7.1.1–7.1.2 описывается формат пролога XML-документа SIMEF.

7.1.1 XML-декларация

SIMEF-документы, передаваемые между SIMEF-совместимыми приложениями, начинаются с декларации XML и должны содержать указание на используемую версию XML. Рекомендуется также указывать используемую спецификацию кодировки.

Таким образом SIMEF-сообщение начинается со следующих данных:

```
<?xml version="1.0" encoding="UTF-8"?>
<simef: SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef"/>
```

При внутреннем обмене SIMEF-совместимые приложения могут опускать декларацию XML для экономии места, добавляя ее только тогда, когда сообщение передается в другую систему (например, в веб-браузер). Такая практика не рекомендуется, если она не может осуществляться без потери информации о версии и кодировке каждого сообщения.

Таким образом разработчики могут позволить анализаторам и диспетчерам отдельно согласовывать конкретное определение типа документа (DTD), которое будет использоваться для обмена сообщениями (стандартное, как показано здесь, или с расширениями), а затем опускать DTD в SIMEF-сообщениях. Метод заключения подобного соглашения не входит в сферу применения настоящей Рекомендации.

7.1.2 Обработка символьных данных SIMEF

В целях обеспечения переносимости в SIMEF-совместимых приложениях не следует использовать кодировку символов, отличную от UTF-8 и UTF-16, и SIMEF-сообщения не должны быть представлены в такой кодировке. В соответствии со стандартом XML, если для SIMEF-сообщения не указана никакая кодировка, то предполагается, что используется UTF-8.

7.1.2.1 Запись символов в виде объектных ссылок

В SIMEF-совместимых приложениях для символов "&", "<", ">", "„" (двойные кавычки) и "‚" (одинарная кавычка) при их написании в данных во избежание любой возможности неправильного толкования рекомендуется использовать форму объектной ссылки.

7.1.2.2 Обработка пробелов

Все элементы SIMEF должны поддерживать атрибут "xml:space".

7.1.2.3 Языки SIMEF

В SIMEF-совместимых приложениях указывается язык, на котором кодируется их содержимое; в общем случае это может быть сделано посредством указания атрибута "xml:lang" для элемента верхнего уровня с разрешением "наследования" этого определения всеми другими элементами.

7.2 Типы данных SIMEF

В XML-сообщении SIMEF все данные выражаются в виде текста, так как XML – это язык форматирования текста. Он выражает сведения о типе атрибутов классов в модели данных. В XML-сообщении SIMEF для каждого типа данных в модели предъявляются конкретные требования к форматированию; эти требования излагаются в настоящем пункте.

7.2.1 Целые числа

Целочисленные атрибуты представляются типом данных INTEGER. Целочисленные данные кодируются в системе Base 10 или Base 16. В целочисленной кодировке Base 10 используются цифры от "0" до "9" и необязательный знак ("+" или "–"). Например, "123", "–456". В целочисленной кодировке Base 16 используются цифры от "0" до "9", буквы от "a" до "f" (или их эквиваленты в верхнем регистре) и приставка в виде символов "0x". Например, "0x1a2b".

7.2.2 Действительные числа

Атрибуты, выражаемые действительными числами (с плавающей запятой), представляются типом данных REAL. Действительные числа кодируются в системе Base 10. Кодировка действительных чисел соответствует функции библиотеки "strtod" Интерфейса переносимых операционных систем (POSIX) 1003.1 [b-IEEE 1003.1]: необязательный знак ("+" или "–"), за которым следует непустая строка десятичных цифр, которая также может содержать десятичный разделитель, и необязательный порядок числа. Порядок числа состоит из буквы "e" или "E", за которой следуют необязательный знак ("+" или "–") и одна или несколько десятичных цифр. Например, "123.45e02", "–567, 89e-03". SIMEF-совместимые приложения должны поддерживать оба десятичных разделителя "." и ",".

7.2.3 Символы и строки

Атрибуты из одного символа представлены типом данных CHARACTER. Атрибуты известной длины, состоящие из нескольких символов, представлены типом данных STRING. К форматированию данных типа character и string не предъявляется никаких особых требований, за исключением того, что для представления специальных символов в них следует использовать ссылки на эти символы.

7.2.3.1 Объектные ссылки символов

В XML-документах определенные символы в некоторых контекстах имеют особое значение. Для включения в один из таких контекстов собственно символа используются специальные ESC-последовательности, называемые объектными ссылками.

Ниже указываются символы, которые иногда нужно записывать в виде ESC-последовательности, и соответствующие им объектные ссылки:

Символ	Объектная ссылка
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&apos;

7.2.3.2 Кодовые ссылки символов

Любой символ, определяемый стандартами [b-ISO/IEC 10646] и Unicode, можно включить в XML-документ с помощью ссылки на этот символ. Ссылка на символ начинается с символов "&" и "#" и оканчивается символом ";". Между этими символами вставляется код соответствующего символа.

Если коду символа предшествует буква "x", он интерпретируется как шестнадцатеричный (с основанием 16); в противном случае код интерпретируется как десятичный (с основанием 10). Например, амперсанд (&) имеет код & или &, а знак "меньше чем" (<) имеет код < или <. С использованием этого метода в документ можно включить любой одно-, двух- или четырехбайтный символ, представленный в стандартах ISO/IEC 10646 и Unicode.

7.2.4 Байты

Двоичные данные представляются типом данных BYTE (или BYTE[]). Все двоичные данные кодируются в системе base64.

7.2.5 Перечислимые типы данных

Перечислимые типы представляются типом данных ENUM и представляют собой упорядоченный список допустимых значений.

7.2.6 Строки даты и времени

Строки даты и времени представляются типом данных DATETIME. Каждая строка даты и времени определяет конкретный момент времени; диапазоны не поддерживаются. Строки даты и времени форматируются в соответствии с подмножеством [b-ISO 8601:2004], как показано ниже. Ссылки на раздел в скобках относятся к положениям стандарта [b-ISO 8601:2004].

7.2.7 Отметки времени NTP

Отметки времени сетевого протокола синхронизации времени (NTP) представляются типом данных NTPSTAMP и подробно описываются в [b-IETF RFC 1305] и [b-IETF RFC 5905]. Отметка времени NTP представляет собой 64-разрядное число с фиксированной запятой без знака. Первые 32 бита содержат целую часть числа, а вторые – дробную. В SIMEF-сообщениях отметки времени NTP кодируются двумя 32-разрядными шестнадцатеричными числами, разделенными точкой ("."). Например, "0x12345678.0x87654321".

7.2.8 Списки портов

Списки портов представляются типом данных PORTLIST и состоят из разделенных запятыми списков номеров (отдельных целых чисел) и диапазонов (N-M означает порты от N до M включительно). В одном списке можно использовать любую комбинацию из отдельных номеров и диапазонов. Например:

"5-25,37,42,43,53,69–119,123-514".

7.2.9 Уникальные идентификаторы

В настоящей Рекомендации используются уникальные идентификаторы двух типов. Оба представляются типом данных STRING. Эти идентификаторы реализуются в виде атрибутов соответствующих XML-элементов и имеют следующие уникальные значения:

1 атрибут Device класса deviceid (пункт 8.2.3.2), если он указан, имеет значение, уникальное по всем анализаторам в среде обнаружения вторжений;

2 значение по умолчанию "0", что указывает на то, что анализатор не способен генерировать уникальные идентификаторы.

Атрибут нескольких классов "ident", если он указан, имеет значение, уникальное по всем сообщениям, отправляемым отдельным анализатором. Значение атрибута "ident" является уникальным для каждой конкретной комбинации данных, идентифицирующих объект, но не для каждого объекта. С объектом может быть связано несколько значений "ident". Например, идентификатор хост-компьютера по имени будет иметь одно значение, идентификатор того же хост-компьютера по адресу – второе, а идентификатор этого хост-компьютера по имени и адресу – третье.

Значение по умолчанию "0", что указывает на то, что анализатор не способен генерировать уникальные идентификаторы.

Описание методов создания уникальных значений этих атрибутов не входит в сферу применения настоящей Рекомендации.

8 Модель данных SIMEF

В этом пункте подробно описываются отдельные компоненты модели данных SIMEF. Предлагаемые схемы модели на языке UML демонстрируют, каким образом эти компоненты связаны друг с другом.

8.1 Общие сведения о модели данных

На рисунке 2 показана связь между основными компонентами модели данных. Классом верхнего уровня является класс SIMEF-Message; каждый тип сообщений представляет собой подкласс этого класса верхнего уровня. Определено два типа сообщений: Connects и Heartbeats. В каждом сообщении для предоставления подробной информации, передаваемой в сообщении, используются подклассы конкретного класса сообщения. Класс сообщений Connect имеет несколько подклассов, таких как devices, policy, source, target и additional data.

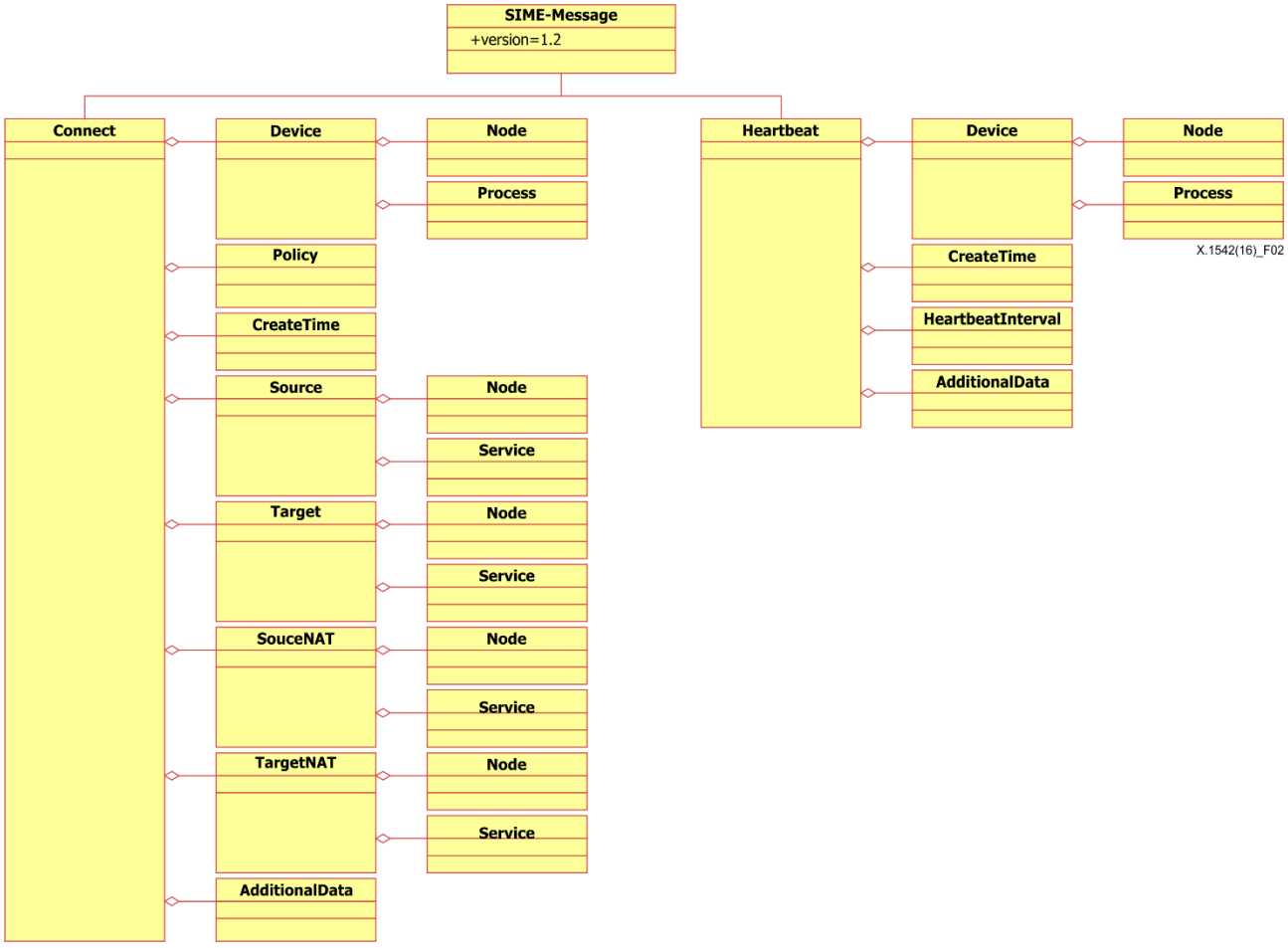

Рисунок 2 – Модель данных SIMEF

8.1.1 Классы SIMEF

Все SIMEF-сообщения являются экземплярами класса SIMEF-Message; Connect и Heartbeat. В этом пункте описываются отдельные классы. См. рисунок 3, таблицу 1 и таблицу 2.

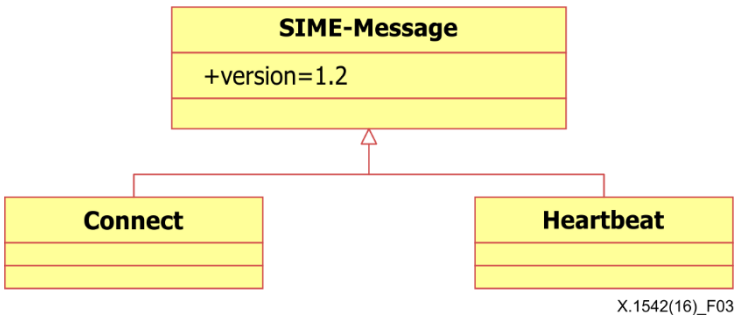

Рисунок 3 – Класс верхнего уровня модели данных SIMEF

Таблица 1 – Атрибуты классов SIMEF

Атрибут	Режим использования	Тип данных	Описание
Version	Обязательный	STRING	Сведения о версии SIMEF, значение по умолчанию 1.2

Таблица 2 – Компоненты классов SIMEF

Класс	Агрегирование	Тип данных	Описание
Connect	Только один		Класс информации о сеансе
Heartbeat	Ноль или один		Класс сведений о состоянии системы, необязательное предоставление

8.2 Классы сообщений

Отдельные классы описываются в подпунктах 8.2.1–8.2.4.

8.2.1 Класс Connect

Класс Connect предназначен для включения информации о сеансе. Он выражает тип журнала, созданного данным соединением в брандмауэре, а также содержит всю информацию о попытках установления как внутренних, так и наружных соединений. См. таблицу 3. В таблице 4 приведены допустимые значения атрибута criticality класса Connect. Класс Connect состоит из нескольких агрегированных классов, как показано на рисунке 4. Сами агрегированные классы описываются в таблице 5.

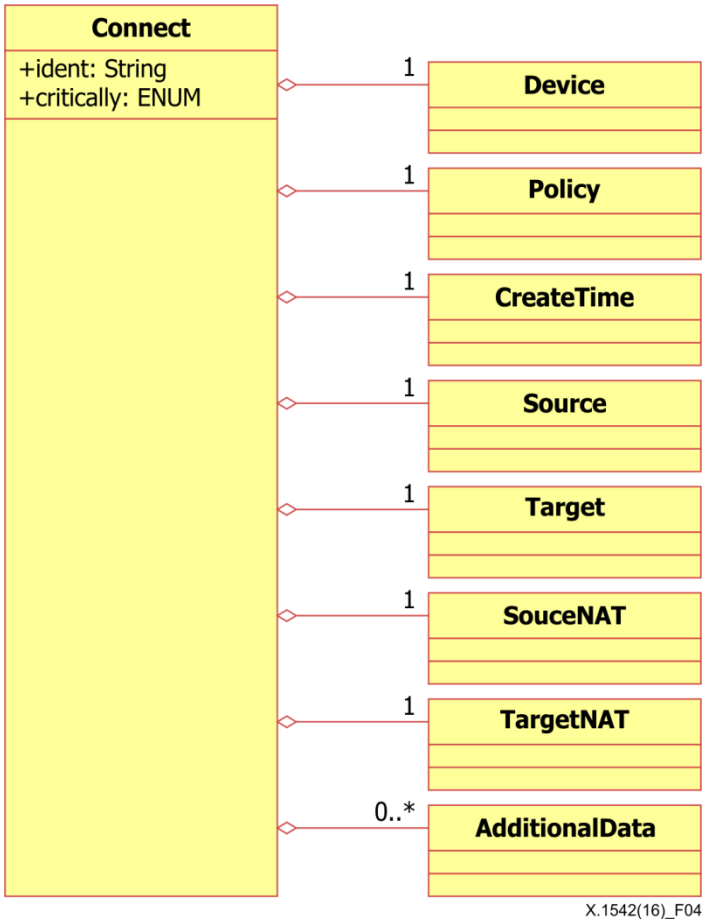

Рисунок 4 – Агрегированные классы в составе класса Connect

Таблица 3 – Атрибуты класса Connect

Атрибут	Режим использования	Тип данных	Описание
ident	Факультативный	STRING	Уникальный идентификатор для информации о доступе
criticality	Факультативный	ENUM	Классификация в соответствии с оценкой события, созданного конкретным соединением. Значение по умолчанию: Unknown

Таблица 4 – Значения атрибута criticality

Значение	Ключевое слово	Определение
0	unknown	Когда влияние данного события неизвестно или не может быть определено
1	normal	Если это обычное соединение
2	suspicious	Если это подозрительное соединение
3	warning	Если данное соединение может быть опасным
4	critical	Если это соединение чувствительно к данному действию

Таблица 5 – Компоненты класса Connect

Класс	Агрегирование	Тип данных	Описание
Device	Только один		Сведения об анализаторе, создающем журнал
Policy	Только один		Сведения о соединении, поступившие в анализатор
CreateTime	Только один	DATETIME	Время создания журнала
Source	Только один		Источник события, вызывающего соединение
Target	Только один		Сведения о месте назначения события, вызывающего соединение
SourceNAT	Только один		Сведения об источнике NAT-события, вызывающего соединение
TargetNAT	Только один		Сведения о месте назначения NAT-события, вызывающего соединение
AdditionalData	Ноль или более		Дополнительная информация, генерируемая детектором, не относящаяся к другим классам

8.2.1.1 Класс Policy

Класс Policy содержит сведения о действии, указывающие, как поступить с сеансом в анализаторе. См. таблицу 5.

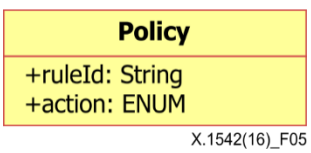

Рисунок 5 – Класс Policy

Допустимые значения атрибутов action класса Policy (см. таблицу 6) приведены в таблице 7.

Таблица 6 – Атрибуты класса Policy

Атрибут	Режим использования	Тип данных	Описание
ruleId	Факультативный	STRING	Уникальный идентификатор правил брандмауэра, создаваемых соединением
action	Факультативный	ENUM	Классификация операции, вызванной соединением, согласно брандмауэру. Значение по умолчанию: Unknown

Таблица 7 – Значения атрибута action

Значение	Ключевое слово	Определение
0	unknown	Если поведение неизвестно
1	pass	Если разрешается соединение
2	block	Если запрещается соединение
3	protect	Если шифруется передаваемый пакет или вставляется код проверки целостности [журнал виртуальной частной сети (VPN)]
4	reject	Если отказано в соединении. Однако при отказе в доступе предоставляются сообщения об ошибке

8.2.2 Класс Heartbeat

Анализаторы используют сообщения Heartbeat для указания диспетчерам своего текущего состояния. Сообщения Heartbeat следует передавать через равные промежутки времени, например каждые 10 минут или каждый час. Получение сообщения Heartbeat от анализатора указывает диспетчеру, что анализатор готов к работе; отсутствие сообщения Heartbeat (или чаще отсутствие некоторого количества последовательных сообщений Heartbeat) указывает на отказ анализатора или сетевого соединения.

Все диспетчеры должны поддерживать получение сообщений Heartbeat; однако анализаторам не обязательно использовать эти сообщения. Разработчики программного обеспечения диспетчеров должны обеспечить возможность его настройки на использование/неиспользование сообщений Heartbeat каждым анализатором. Сообщение Heartbeat состоит из нескольких агрегированных классов, как показано на рисунке 6.

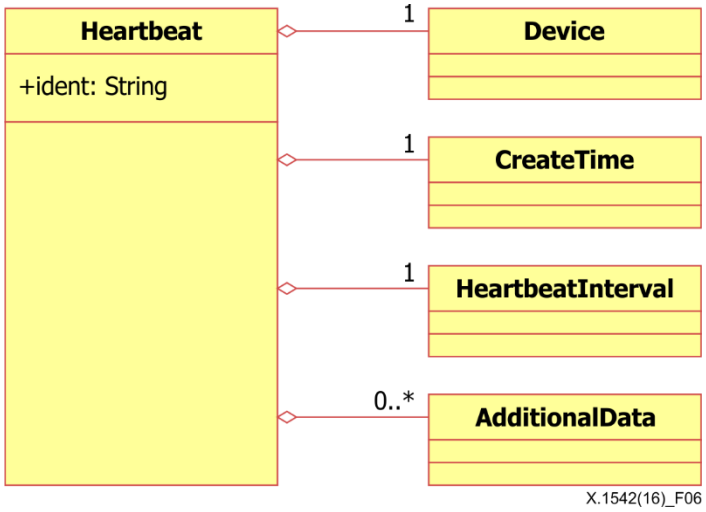

Рисунок 6 – Агрегированные классы в составе класса Heartbeat

Сведения об атрибуте и компонентах класса Heartbeat приведены соответственно в таблице 8 и таблице 9.

Таблица 8 – Атрибут класса Heartbeat

Атрибут	Режим использования	Тип данных	Описание
ident	Факультативный	STRING	Уникальный идентификатор сообщения Heartbeat

Таблица 9 – Компоненты класса Heartbeat

Класс	Агрегирование	Тип данных	Описание
Device	Только один		Информация, идентифицирующая анализатор – источник сообщения heartbeat
CreateTime	Только один	DATETIME	Время создания сообщения heartbeat
HeartbeatInterval	Только один	INTEGER	Интервал в секундах, с которым создаются сообщения heartbeat
AdditionalData	Ноль или более		Информация, включаемая анализатором, которая не вписывается в модель данных

8.2.3 Базовые классы

Основную часть классов Connect и Heartbeat составляют базовые классы (Device, CreateTime, Source, Target, SourceNAT, TargetNAT и AdditionalData), как показано на рисунке 7. В этом пункте описываются отдельные классы.

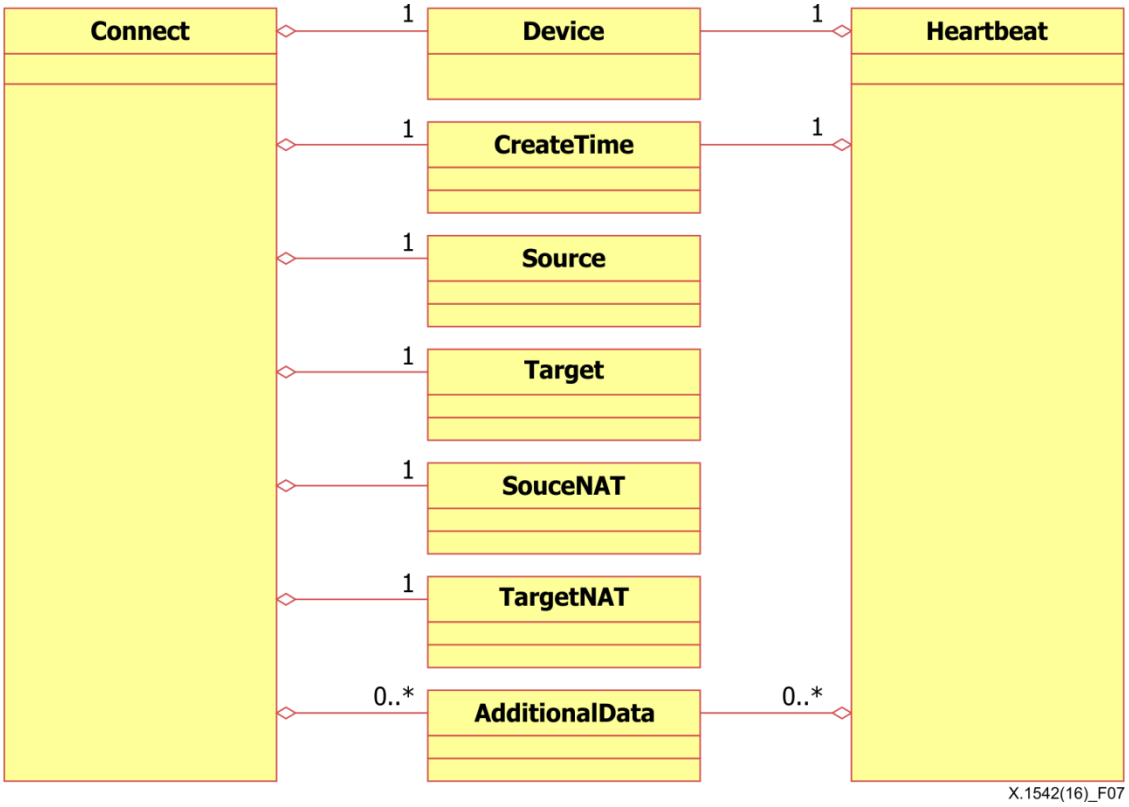

Рисунок 7 – Базовые классы

8.2.3.1 Класс Device

Класс Device определяет анализатор, из которого исходит сообщение Connect или Heartbeat. В каждом сообщении Connect или Heartbeat может быть указано только одно устройство, и это должно быть устройство – источник сообщения connect или heartbeat.

Класс Device состоит из трех агрегированных классов, как показано на рисунке 8.

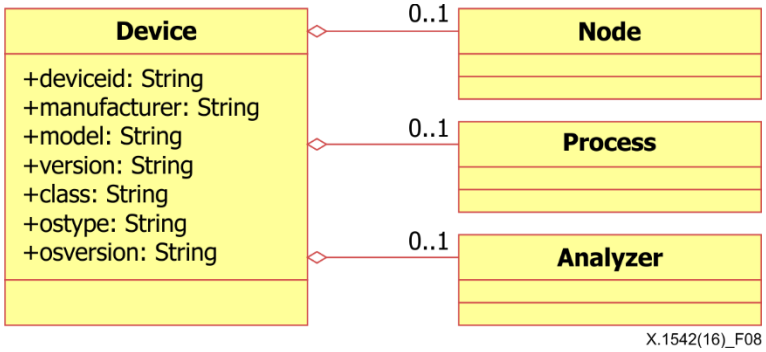

Рисунок 8 – Агрегированные классы в составе класса Device

Класс Device имеет семь атрибутов, как указано в таблице 10.

Таблица 10 – Атрибуты класса Device

Атрибут	Режим использования	Тип данных	Описание
deviceid	Факультативный	STRING	Уникальный идентификатор устройства. Если устройство использует атрибуты "ident" других классов для представления уникальных идентификаторов этих объектов, то оно также должно указать действительный атрибут "deviceid"
Manufacturer	Факультативный	STRING	Производитель программного или аппаратного обеспечения устройства
Model	Факультативный	STRING	Наименование/номер модели программного или аппаратного обеспечения устройства
Version	Факультативный	STRING	Номер версии программного или аппаратного обеспечения устройства
Class	Факультативный	STRING	Класс программного или аппаратного обеспечения устройства
Ostype	Факультативный	STRING	Название операционной системы
osversion	Факультативный	STRING	Версия операционной системы

Что касается атрибута ostype в системах, совместимых с POSIX 1003.1, это значение, возвращаемое в свойстве utsname.sysname по системному вызову uname() или по команде "uname–s".

Что касается атрибута osversion в системах, совместимых с POSIX 1003.1, это значение, возвращаемое в свойстве utsname.release по системному вызову uname() или по команде "uname–r".

Содержание атрибутов "manufacturer", "model", "version" и "class" зависит от поставщика, но они могут использоваться вместе для определения различных типов анализаторов.

Агрегированные классы, составляющие класс Device, описываются в таблице 11.

Таблица 11 – Компоненты класса Device

Класс	Агрегирование	Тип данных	Описание
Node	Ноль или один		Сведения о хост-компьютере или устройстве, в котором находится данный анализатор (сетевой адрес, сетевое имя и др.)
Process	Ноль или один		Сведения о процессе, в котором работает данный анализатор
Analyser	Ноль или один		Сведения об анализаторе, через который могло прийти сообщение

8.2.3.2 Класс CreateTime

Класс CreateTime используется для указания текущей даты и времени в устройстве. Если эти данные затем используются для корректировки времени в элементах <CreateTime> и < NTP timestamps>, то должны корректироваться и отметки времени NTP.

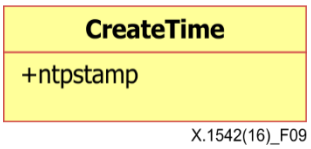

Рисунок 9 – Класс CreateTime

Атрибут класса CreateTime показан в таблице 12.

Таблица 12 – Атрибут класса CreateTime

Атрибут	Режим использования	Тип данных	Описание
ntpstamp	Обязательный	ntpstamp	Сведения о текущем времени в устройстве.

8.2.3.3 Класс Source

Класс Source содержит сведения о возможном(ых) источнике(ах) события(й), инициировавш(их) сеанс. Событие может иметь более одного источника (например, при распределенных воздействиях, вызывающих отказ в обслуживании).

Класс Source состоит из трех агрегированных классов, как показано на рисунке 10.

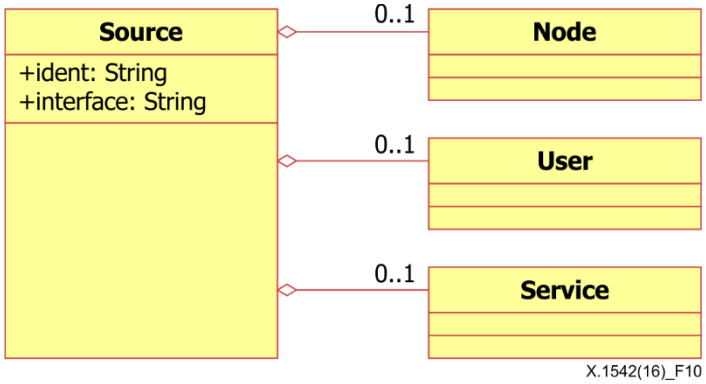

Рисунок 10 – Агрегированные классы в составе класса Source

Класс Source имеет два атрибута, которые указаны в таблице 13.

Таблица 13 – Атрибуты класса Source

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор данного источника.
Interface	Факультативный	STRING	Может использоваться сетевым устройством с несколькими интерфейсами для указания интерфейса, обнаружившего этот источник.

Агрегированные классы, составляющие класс Source, описываются в таблице 14.

Таблица 14 – Компоненты класса Source

Класс	Агрегирование	Тип данных	Описание
Node	Ноль или один		Сведения о хост-компьютере или устройстве, предположительно вызывающем события (сетевой адрес, сетевое имя и т. д.).
User	Ноль или один		Сведения о пользователе, предположительно вызывающем события.
Service	Ноль или один		Сведения о сетевой службе, участвовавшей в событии(ях).

8.2.3.4 Класс Target

Класс Target содержит сведения о возможной(ых) цели(ях) события(й), инициировавшего(их) сеанс. Событие может иметь более одной цели (например, в случае зондирования портов).

Класс Target состоит из трех агрегированных классов, как показано на рисунке 11.

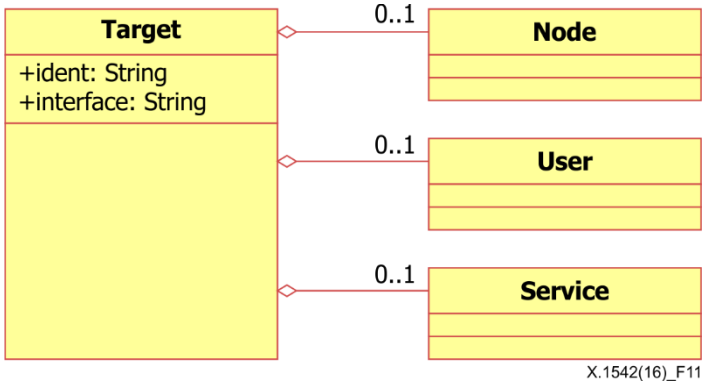

Рисунок 11 – Агрегированные классы в составе класса Target

Класс Target имеет два атрибута, как указано в таблице 15.

Таблица 15 – Атрибуты класса Target

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор данной цели
Interface	Факультативный	STRING	Может использоваться сетевым устройством с несколькими интерфейсами для указания интерфейса, обнаружившего эту цель

Агрегированные классы, составляющие класс Target, описываются в таблице 16.

Таблица 16 – Компоненты класса Target

Класс	Агрегирование	Тип данных	Описание
Node	Ноль или один		Сведения о хост-компьютере или устройстве, на которое направлены события (сетевой адрес, сетевое имя и т. д.)
User	Ноль или один		Сведения о пользователе, на которого направляются события
Service	Ноль или один		Сведения о сетевой службе, участвовавшей в событиях

8.2.3.5 Класс SourceNAT

Класс SourceNAT содержит сведения о возможном(ых) источнике(ах) события(й) NAT, инициировавшего(их) сеанс. Событие может иметь более одного источника, преобразованного с помощью NAT.

Класс SourceNAT состоит из трех агрегированных классов, как показано на рисунке 12.

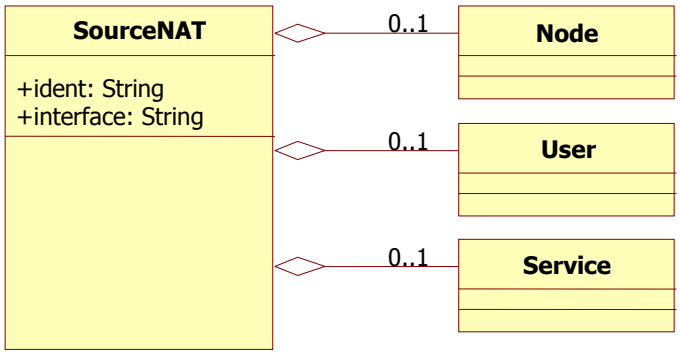

Рисунок 12 – Агрегированные классы в составе класса SourceNAT

Класс Source имеет два атрибута, как указано в таблице 17.

Таблица 17 – Атрибуты класса SourceNAT

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор данного источника, преобразованного с помощью NAT
Interface	Факультативный	STRING	Может использоваться сетевым устройством с несколькими интерфейсами для указания интерфейса, обнаружившего этот источник, преобразованный с помощью NAT

Агрегированные классы, составляющие класс SourceNAT, описываются в таблице 18.

Таблица 18 – Компоненты класса SourceNAT

Класс	Агрегирование	Тип данных	Описание
Node	Ноль или один		Сведения о хост-компьютере или устройстве, предположительно вызывающем события (сетевой адрес, сетевое имя и т. д.)
User	Ноль или один		Сведения о пользователе, предположительно вызывающем событие(я)
Service	Ноль или один		Сведения о сетевой службе, участвовавшей в событии(ях)

8.2.3.6 Класс TargetNAT

Класс TargetNAT содержит сведения о возможной(ых) цели(ях) события(й) NAT, инициировавшего(их) сеанс. Событие может иметь более одной цели, преобразованной с помощью NAT.

Класс TargetNAT состоит из трех агрегированных классов, как показано на рисунке 13.

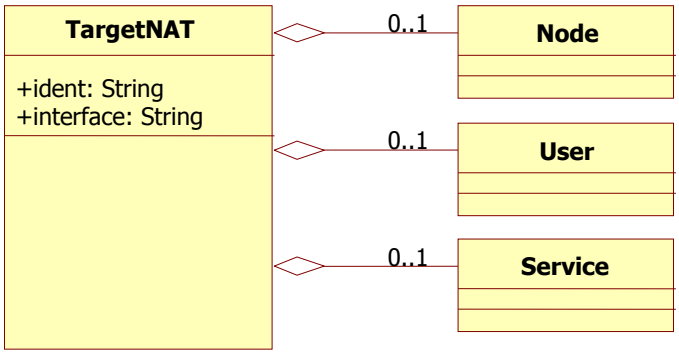

Рисунок 13 – Агрегированные классы в составе класса TargetNAT

Класс TargetNAT имеет два атрибута, как указано в таблице 19.

Таблица 19 – Атрибуты класса TargetNAT

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор данной цели, преобразованной с помощью NAT
Interface	Факультативный	STRING	Может использоваться сетевым устройством с несколькими интерфейсами для указания интерфейса, обнаружившего эту цель, преобразованную с помощью NAT

Агрегированные классы, составляющие класс Target, описываются в таблице 20.

Таблица 20 – Компоненты класса TargetNAT

Класс	Агрегирование	Тип данных	Описание
Node	Ноль или один		Сведения о хост-компьютере или устройстве, на которое направляется(ются) событие(я) (сетевой адрес, сетевое имя и т. д.)
User	Ноль или один		Сведения о пользователе, на которого направляется(ются) событие(я)
Service	Ноль или один		Сведения о сетевой службе, участвовавшей в событии(ях)

8.2.3.7 Класс AdditionalData

Класс AdditionalData используется для предоставления сведений, которые не могут быть представлены в модели данных SIMEF. Класс AdditionalData можно использовать для предоставления простых данных (целые числа, строки и т. д.) в тех случаях, когда необходимо передать лишь небольшой объем дополнительной информации; его также можно использовать для расширения модели данных и DTD, поддерживающего передачу сложных данных (например, заголовков пакетов).

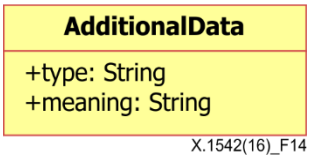

Рисунок 14 – Класс AdditionalData

Класс AdditionalData имеет два атрибута, как указано в таблице 21.

Таблица 21 – Атрибуты класса AdditionalData

Атрибут	Режим использования	Тип данных	Описание
Type	Обязательный	ENUM	Тип данных, описывающий значение содержимого элемента. Значение по умолчанию: string
Meaning	Факультативный	STRING	Строка, описывающая значение содержимого элемента

В таблице 22 приведены типы данных, представленных классом AdditionalData, и допустимые значения атрибута Type.

Таблица 22 – Значения атрибута Type

Значение	Ключевое слово	Определение
0	boolean	Этот элемент содержит логическое значение, то есть строки "true" или "false"
1	byte	Этот элемент содержит один 8-битный байт
2	character	Этот элемент содержит один символ
3	date-time	Этот элемент содержит строку со значением даты и времени
4	integer	Этот элемент содержит целое число
5	ntpstamp	Этот элемент содержит отметку времени NTP
6	portlist	Этот элемент содержит список портов
7	real	Этот элемент содержит действительное число
8	string	Этот элемент содержит строку
9	Byte-string	Это элемент byte[]
10	xml	Этот элемент содержит данные с XML-тегами

Эти значения класса AdditionalData зависят от поставщика/реализации; метод, позволяющий диспетчерам разбираться в передаваемых анализаторами строках, не входит в сферу применения настоящей Рекомендации.

8.2.4 Вспомогательные классы

Вспомогательные классы составляют основную часть базовых классов и используются всеми этими классами.

8.2.4.1 Класс Node

Класс Node используется для идентификации хост-компьютеров и других сетевых устройств (маршрутизаторов, коммутаторов и т. д.).

Класс Node состоит из трех агрегированных классов, как показано на рисунке 15. Атрибуты, значения атрибута Type и компоненты класса Node приведены в таблице 23, таблице 24 и таблице 25 соответственно.

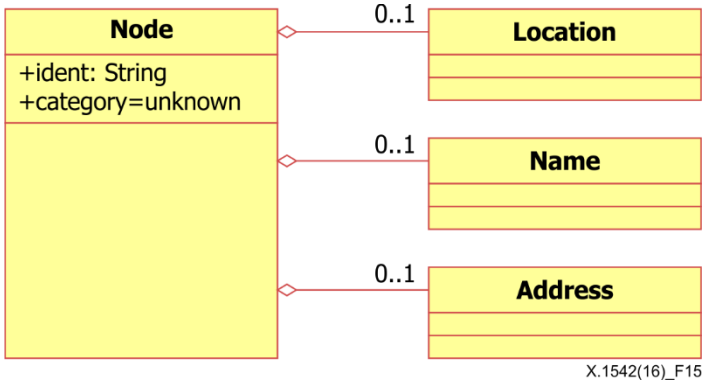

Рисунок 15 – Агрегированные классы в составе класса Node

Таблица 23 – Атрибуты класса Node

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор данного узла; см. пункт 7.2.9.
Category	Факультативный	ENUM	"Домен", из которого была получена информация об имени. Значение по умолчанию = unknown

Таблица 24 – Значения атрибута Type

Значение	Ключевое слово	Определение
0	Unknown	Домен неизвестен или не имеет отношения к данному вопросу
1	ads	Расширенная служба каталогов Windows 2000
2	afs	Файловая система Andrew (Transarc)
3	coda	Распределенная файловая система Coda
4	dfs	Распределенная файловая система (IBM)
5	dns	Система доменных имен
6	hosts	Файлы в локальных хост-компьютерах
7	kerberos	Область Kerberos
8	nds	Служба каталогов Novell
9	nis	Сетевые информационные службы (Sun)
10	nisplus	Сетевые информационные службы плюс (Sun)
11	nt	Домен Windows NT
12	wfw	Windows для рабочих групп

Таблица 25 – Компоненты класса Node

Класс	Агрегирование	Тип данных	Описание
Location	Ноль или один	STRING	Местоположение оборудования
Name	Ноль или один	STRING	Название оборудования. Эта информация предоставляется при отсутствии информации об адресе.
Address	Ноль или более		Сетевой или аппаратный адрес оборудования. Если название (см. выше) не указано, должен быть указан хотя бы один адрес.

8.2.4.2 Класс Address class

Класс Address используется для представления сетевых адресов, адресов оборудования и адресов приложений.

Класс Address состоит из двух агрегированных классов, как показано на рисунке 16.

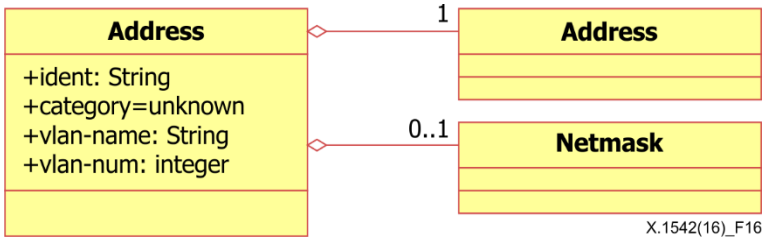

Рисунок 16 – Агрегированные классы в составе класса Address

Атрибуты, значения атрибута Type и компоненты класса Address приведены в таблице 26, таблице 27 и таблице 28 соответственно.

Таблица 26 – Атрибуты класса Address

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор адреса; см. пункт 7.2.9
Category	Факультативный	ENUM	Тип представляемого адреса. Ниже приведены допустимые значения этого атрибута. Значение по умолчанию: unknown
Vlan-name	Факультативный		Имя локальной вычислительной сети (ЛВС) (виртуальной ЛВС), к которой относится адрес
Vlan-num	Факультативный	INTEGER	Номер ЛВС (виртуальной ЛВС), к которой относится адрес

Таблица 27 – Значения атрибута Type

Значение	Ключевое слово	Определение
0	unknown	Тип адреса неизвестен
1	atm	Адрес сети на основе асинхронного режима передачи
2	e-mail	Адрес электронной почты ([b-IETF RFC 2822])
3	lotus-notes	Адрес электронной почты Lotus Notes
4	Mac	Адрес управления доступом к среде передачи (MAC)
5	Sna	Адрес совместно используемой сетевой архитектуры (SNA) IBM
6	Vm	Адрес электронной почты IBM VM ("PROFS")
7	ipv4-addr	Адрес узла IPv4 в виде десятичного числа с фиксированной точкой (a.b.c.d)
8	ipv4-addr-hex	Адрес узла IPv4 в шестнадцатеричной записи
9	ipv4-net	Сетевой адрес IPv4 в виде десятичного числа с фиксированной точкой, косая черта, количество значимых битов (a.b.c.d/nn)
10	ipv4-net-mask	Сетевой адрес IPv4 в виде десятичного числа с фиксированной точкой, косая черта, маска сети в виде десятичного числа с фиксированной точкой (a.b.c.d./w.x.y.z)
11	ipv6-addr	Адрес узла IPv6
12	ipv6-addr-hex	Адрес узла IPv6 в шестнадцатеричной записи
13	ipv6-net	Сетевой адрес IPv6, косая черта, количество значащих битов
14	ipv6-net-mask	Сетевой адрес IPv6, косая черта, маска сети

Таблица 28 – Компоненты класса Address

Класс	Агрегирование	Тип данных	Описание
Address	Только один	STRING	Информация об адресе. Формат этих данных определяется атрибутом category
Netmask	Ноль или один	STRING	Маска сети для адреса при необходимости

8.2.4.3 Класс User

Класс User используется для описания пользователей. Он применяется главным образом в качестве класса-"контейнера" для агрегированного класса UserId, как показано на рисунке 17.

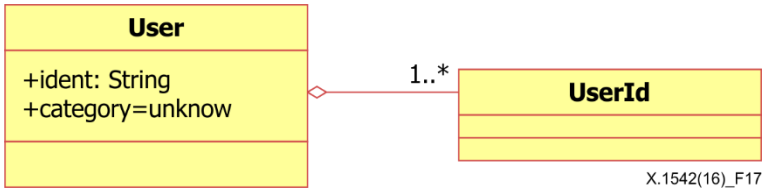

Рисунок 17 – Агрегированные классы в составе класса User

Атрибуты, значения атрибута Type и компоненты класса User приведены в таблице 29, таблице 30 и таблице 31 соответственно.

Таблица 29 – Атрибуты класса User

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор пользователя; см. пункт 7.2.9.
Category	Факультативный	ENUM	Тип представляемого пользователя. Ниже приведены допустимые значения этого атрибута. Значение по умолчанию = unknown.

Таблица 30 – Значения атрибута Type

Значение	Ключевое слово	Определение
0	unknown	Тип пользователя неизвестен
1	application	Пользователь приложения
2	os-device	Пользователь операционной системы или устройства

Таблица 31 – Компоненты класса User

Класс	Агрегирование	Тип данных	Описание
UserId	Один или несколько		Идентификатор пользователя в соответствии с его атрибутом Type

8.2.4.3.1 Класс UserId

Класс UserId содержит конкретную информацию о пользователе. Внутри класса User может применяться несколько идентификаторов UserId для указания попыток перехода от одного пользователя к другому или для предоставления полной информации о привилегиях пользователя (или процесса).

Класс UserId состоит из двух агрегированных классов, как показано на рисунке 18.

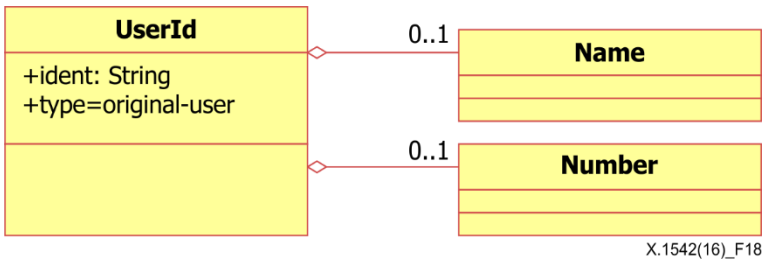

Рисунок 18 – Агрегированные классы в составе класса UserId

Атрибуты и значения атрибута Type класса UserId приведены в таблице 32 и таблице 33 соответственно.

Таблица 32 – Атрибуты класса UserId

Атрибут	Режим использования	Тип данных	Описание
ident	Факультативный	STRING	Уникальный идентификатор для идентификатора пользователя; см. пункт 7.2.9.
type	Факультативный	ENUM	Тип представляемой информации о пользователе. Ниже приведены допустимые значения этого атрибута. Значение по умолчанию =original-user

Таблица 33 – Значения атрибута Type

Значение	Ключевое слово	Определение
0	current-user	Текущий идентификатор пользователя, применяемый пользователем или процессом.
1	original-user	Действительный идентификатор пользователя или процесса, к которому относится сообщение. Это значение следует использовать в тех системах, которые a) выполняют какую-либо проверку и b) поддерживают извлечение идентификатора пользователя из маркера "audit id". В тех системах, которые этого не поддерживают и в которых пользователь зарегистрирован, следует использовать "login id".
2	target-user	Идентификатор пользователя, за которого пользователь или процесс пытается себя выдать. Это применимо, например, в Unix-системах, когда пользователь пытается использовать протоколы "su", "rlogin", "telnet" и т. д.
3	user-privs	Еще один идентификатор пользователя, которым может воспользоваться пользователь или процесс, или идентификатор пользователя, связанный с разрешением на доступ к файлу. Можно применять несколько элементов UserId этого типа для указания списка привилегий.
4	current-group	Текущий идентификатор группы (в соответствующих случаях), применяемый пользователем или процессом.
5	group-privs	Еще один идентификатор группы, которым может воспользоваться группа или процесс, или идентификатор группы, связанный с разрешением на доступ к файлу. Например, в Unix-системах, производных от системы распространения программного обеспечения Беркли (BSD), несколько элементов UserId этого типа можно использовать для включения всех идентификаторов групп в "список групп".
6	other-privs	Не применяется в контекстах пользователя, группы или процесса; применяется только в контексте файла. Назначенные пользователям разрешения на доступ к файлу, не совпадающие с разрешениями на доступ к файлу пользователя или группы.

Класс UserId составляют агрегированные классы, перечисленные в таблице 34.

Таблица 34 – Компоненты класса UserId

Класс	Агрегирование	Тип данных	Описание
Name	Ноль или один	STRING	Имя пользователя или группы.
Num	Ноль или один	INTERGER	Номер пользователя или группы.

8.2.4.4 Класс Process

Класс Process используется для описания процессов, выполняемых в источниках, целевых узлах и анализаторах.

Класс Process состоит из пяти агрегированных классов, как показано на рисунке 19.

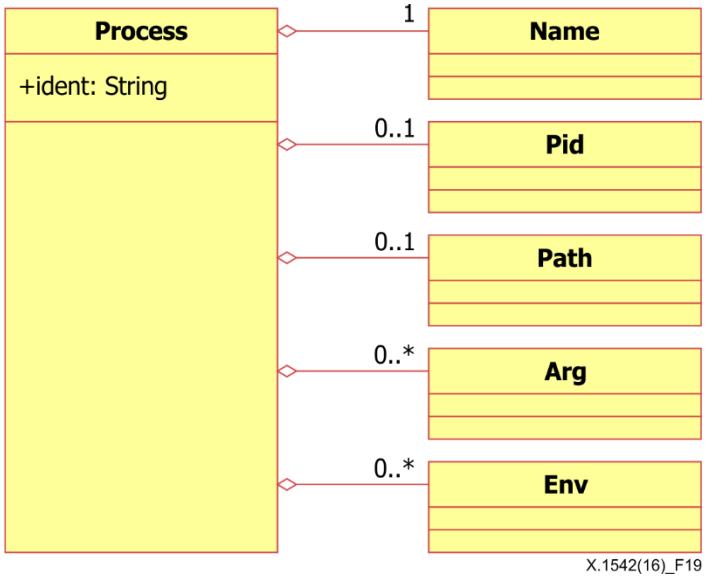

Рисунок 19 – Агрегированные классы в составе класса Process

Класс Process имеет единственный атрибут (см. таблицу 35).

Таблица 35 – Атрибут класса Process

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор процесса; см. пункт 7.2.9.

Класс Process составляют агрегированные классы, перечисленные в таблице 36.

Таблица 36 – Компоненты класса Process

Класс	Агрегирование	Тип данных	Описание
Name	Только один	STRING	Имя выполняемой программы.
Pid	Ноль или один	INTEGER	Идентификатор процесса.
Path	Ноль или один	STRING	Полный путь выполняемой программы.
Arg	Ноль или более	STRING	Аргумент командной строки программы.
Env	Ноль или более	STRING	Строка описания конфигурации, связанная с процессом; обычно в формате "VARIABLE = value".

В классе Process имя класса – это короткое имя, и может быть указано несколько аргументов в нескольких элементах arg. Может быть указано несколько строк описания конфигурации в нескольких элементах env.

8.2.4.5 Класс Service

Класс Service служит для описания сетевых служб в исходных и целевых узлах. Он позволяет идентифицировать сетевые службы по именам, портам, списку портов и протоколу. Когда класс Service выступает в качестве агрегированного класса в составе класса Source, следует понимать, что речь идет о службе, от которой исходит интересующая нас деятельность, и что информация класса

Node, Process и User, содержащаяся в классе Source, "относится" и к этой службе. Аналогично когда класс Service выступает в качестве агрегированного класса в составе класса Target, следует понимать, что речь идет о службе, на которую направлена интересующая нас деятельность, и что информация класса Node, Process и User, содержащаяся в классе Target, "относится" и к этой службе. Если класс Service присутствует в обоих классах Source и Target, то информация в обоих местах должна быть одинаковой. Если информация в обоих местах одинакова и разработчики хотят, чтобы она отражалась только в одном месте, они должны указать этот класс как агрегированный класс в составе класса Target.

Класс Service состоит из четырех агрегированных классов, как показано на рисунке 20.

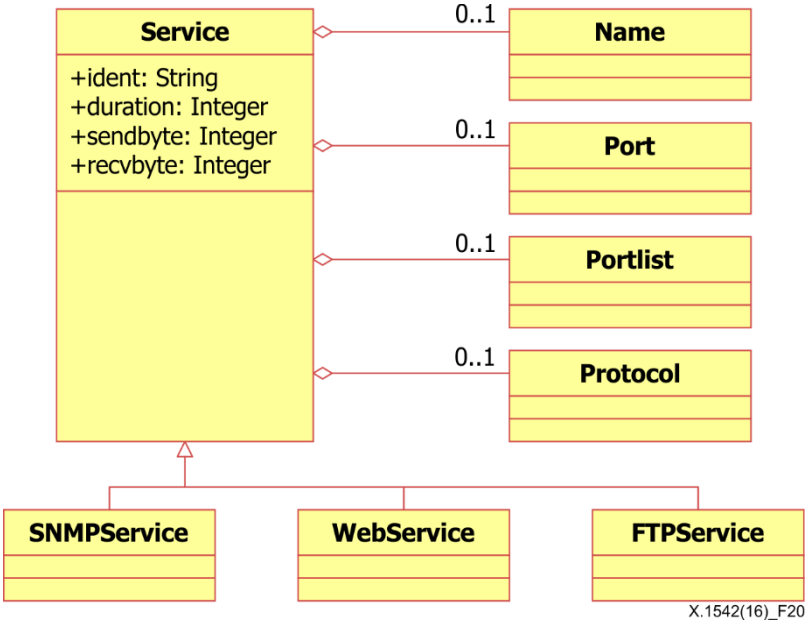

Рисунок 20 – Агрегированные классы в составе класса Service

Класс Service имеет четыре атрибута, которые перечислены в таблице 37.

Таблица 37 – Атрибуты класса Service

Атрибут	Режим использования	Тип данных	Описание
Ident	Факультативный	STRING	Уникальный идентификатор службы; см. пункт 7.2.9.
Duration	Факультативный	INTEGER	Время соединения
Sendbyte	Факультативный	INTEGER	Количество байтов, отправленных после установления соединения
RecvByte	Факультативный	INTEGER	Количество байтов, полученных после установления соединения

Класс Service составляют агрегированные классы, перечисленные в таблице 38.

Таблица 38 – Компоненты класса Service

Класс	Агрегирование	Тип данных	Описание
Name	Ноль или один	STRING	Имя службы. По возможности следует использовать имя из списка известных портов полномочного органа присвоения номеров интернета (IANA).
Port	Ноль или один	INTEGER	Используемый номер порта.
Portlist	Ноль или один	PORTLIST	Список используемых номеров портов; см. правила форматирования в пункте 7.2.8.
Protocol	Ноль или один	STRING	Дополнительная информация об используемом протоколе.

8.2.4.5.1 Класс WebService

Класс WebService содержит дополнительную информацию, относящуюся к веб-трафику.

Класс WebService состоит из четырех агрегированных классов, как показано на рисунке 21.

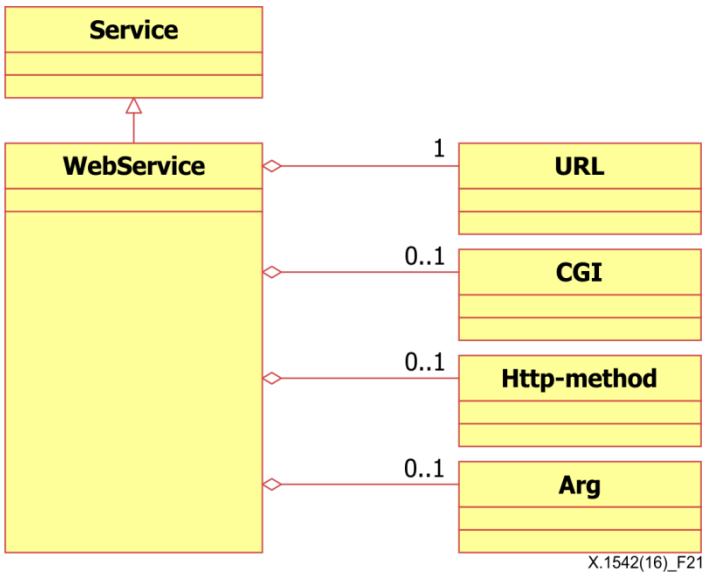

Рисунок 21 – Агрегированные классы в составе класса WebService

Составляющие класс WebService агрегированные классы перечислены в таблице 39.

Таблица 39 – Компоненты класса WebService

Класс	Агрегирование	Тип данных	Описание
URL	Только один	STRING	Унифицированный указатель ресурса (URL) в запросе.
CGI	Ноль или один	STRING	Сценарий общего шлюзового интерфейса (CGI) в запросе – без аргументов.
Http-method	Ноль или один	STRING	Используемый в запросе метод (PUT, GET) протокола гипертекстовой передачи (HTTP).
Arg	Ноль или один	STRING	Аргументы сценария CGI.

8.2.4.5.2 Класс SNMPService

Класс SNMPService содержит дополнительную информацию, касающуюся трафика простого протокола управления сетью (SNMP).

Класс SNMPService состоит из восьми агрегированных классов, как показано на рисунке 22.

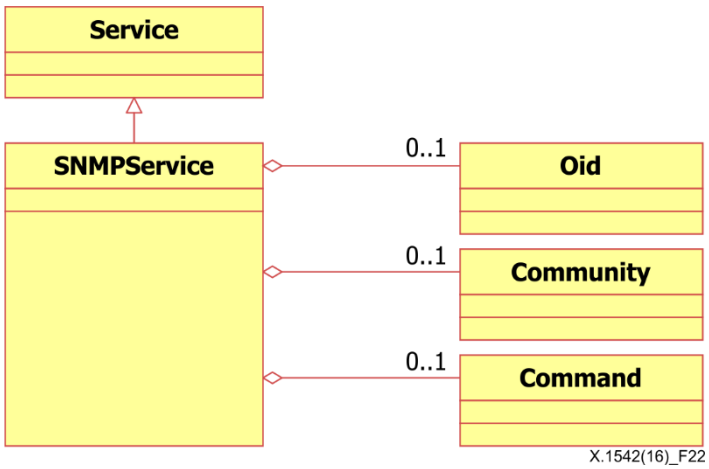

Рисунок 22 – Агрегированные классы в составе класса SNMPService

Класс SNMPService составляют агрегированные классы, перечисленные в таблице 40.

Таблица 40. Компоненты класса SNMPService

Класс	Агрегирование	Тип данных	Описание
Oid	Ноль или один	STRING	Идентификатор объекта в запросе.
Community	Ноль или один	STRING	Строка сообщества объекта.
Command	Ноль или один	STRING	Команда, переданная в SNMP-сервер (GET, SET и т. д.).

8.2.4.5.3 Класс FTPService

Класс FTPService содержит дополнительную информацию, относящуюся к трафику протокола передачи файлов (FTP).

Класс FTPService состоит из двух агрегированных классов, как показано на рисунке 23.

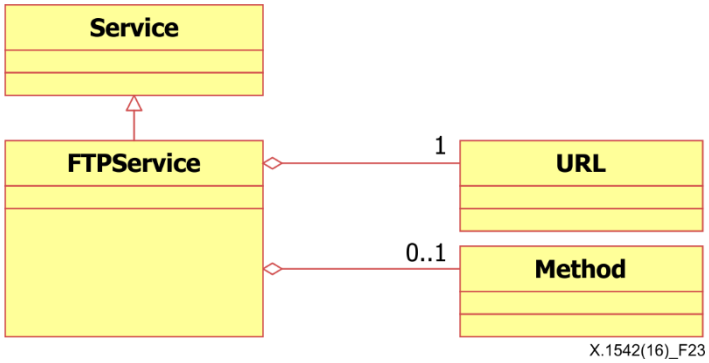

Рисунок 23 – Агрегированные классы в составе класса FTPService

Класс FTPService составляют агрегированные классы, перечисленные в таблице 41.

Таблица 41 – Компоненты класса FTPService

Класс	Агрегирование	Тип данных	Описание
URL	Только один	STRING	URL-адрес в запросе.
Method	Ноль или один	STRING	Метод FTP (PUT, GET), используемый в запросе.

9 Соображения по вопросам безопасности

В этом пункте обсуждаются некоторые соображения по вопросам безопасности, которые необходимо принимать во внимание при реализации SIMEF.

В настоящей Рекомендации описывается информационная модель формата обмена информационными сообщениями сеанса (SIMEF) и представляется соответствующая модель данных, описываемая с помощью XML-схемы. SIMEF определяет представление модели данных для совместного использования информации журнала сеансов транспортного уровня, относящейся к централизованной системе управления безопасностью сети и обмена информацией по безопасности.

Хотя нет никаких проблем по вопросам безопасности, непосредственно связанных с форматом этих данных, сами данные могут содержать важные в отношении обеспечения безопасности сведения, конфиденциальность, целостность или доступность которых может нуждаться в защите.

В настоящей Рекомендация предполагается, что системы, используемые для сбора, передачи, обработки и хранения этих данных, должны быть защищены от несанкционированного использования и что сами данные должны быть защищены от несанкционированного доступа. Средства достижения такой защиты не входят в сферу применения этой Рекомендации.

Дополнение I

Пример и схема SIMEF

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В этом Дополнении приводится пример XML-схемы для модели SIMEF. Следующие примеры представляют собой XML-схему и схему SYSLOG для кодирования информации о сеансе в SIMEF-модель.

I.1 Схема SIMEF

I.1.1 XML-схема

```
  <?xml version="1.0" encoding="UTF-8"?>

  <simef:SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef/">
       <Connect ident="1008380" criticality="normal">
          <Device Deviceid="TTA-FW" model="FW1000">
             <Node>
                <Address category="ipv4-addr">
                  <address>1.1.1.1</address>
                </Address>
             </Node>
          </Device>
          <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                    2010-08-18T15:41:28+00:00
          </CreateTime>
          <Policy Ruleid="45" action="pass"></Policy>
             <Source>
             <Node>
                <Address category="ipv4-addr">
                  <address>2.2.2.2</address>
                </Address>
             </Node>
             <Service duration="9" size="144">
                <port>38168</port>
                <protocol>17</protocol>
             </Service>
          </Source>
          <Target>
             <Node>
                <Address category="ipv4-addr">
                  <address>3.3.3.3</address>
                </Address>
             </Node>
             <Service duration="9" size="0">
                <name>dns</name>
                <port>53</port>
                <protocol>17</protocol>
             </Service>
          </Target>
          <Classification origin="vendor-specific">
             <name>45</name>
          </Classification>
       </Connect>
</simef:SIMEF-Message>
```

I.1.2 Схема SYSLOG

```
      2014-03-18 15:41:28 Local0.Notice 1.1.1.1 TTA: TTA-FW device_id= TTA
   [Root]system-notification-00257(traffic): start_time="2014-03-18 15:41:19"
  duration=9 policy_id=45 service=dns proto=17 src zone=Untrust dst zone=Trust
action=Permit sent=144 rcvd=0 src=2.2.2.2 dst=3.3.3.3 src_port=38168 dst_port=53
         src-xlated ip=2.2.2.2 port=38168 dst-xlated ip=3.3.3.3 port=53
                 session_id=1008380 reason=Close - AGE OUT<000>
```

I.2 Примеры SIMEF

I.2.1 Разрешение брандмауэра

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008380" criticality="1">
              <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
                            </Address>
                     </Node>
              </Device>
              <Policy Ruleid="45" action="1"></Policy>
              <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                     2014-03-18T15:41:28+00:00
              </CreateTime>
              <Source>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>2.2.2.2</address>
                            </Address>
                     </Node>
                      <Service duration="9" size="144">
                            <port>38168</port>
                            <protocol>17</protocol>
                     </Service>
              </Source>
              <Target>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>3.3.3.3</address>
                            </Address>
                     </Node>
                     <Service duration="9" size="0">
                            <name>dns</name>
                            <port>53</port>
                            <protocol>17</protocol>
                     </Service>
              </Target>
              <Classification origin="2">
                     <name>45</name>
              </Classification>
       </Connect>
</SIMEF-Message>
```

I.2.2 Журнал VPN

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
	<Connect ident="1008057" criticality="1">
		<Device Deviceid="TTA-VPN" manufacturer="TTA" model="VPN1000">
			<Node>
				<Address category="ipv4-addr">
					<address>1.1.1.1</address>
				</Address>
			</Node>
		</Device>
		<Policy ruleid="700" action="3"></Policy>
		<CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
			2014-03-19T12:51:22+00:00
		</CreateTime>
		<Source>
			<Node>
				<Address category="ipv4-addr">
					<address>2.2.2.2</address>
				</Address>
			</Node>
			<Service duration="41" size="16905">
				<port>59078</port>
				<protocol>TCP</protocol>
			</Service>
		</Source>
		<Target>
			<Node>
				<Address category="ipv4-addr">
					<address>3.3.3.3</address>
				</Address>
			</Node>
			<Service duration="41" size="1448">
				<name>junos-http</name>
				<port>80</port>
				<protocol>TCP</protocol>
			</Service>
		</Target>
		<Classification origin="2">
			<name>700</name>
		</Classification>
	</Connect>
</SIMEF-Message>
```

I.2.3 Журнал NAT

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
	<Connect ident="1009632" criticality="1">
		<Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
		<Node>
				<Address category="ipv4-addr">
					<address>1.1.1.1</address>
				</Address>
			</Node>
		</Device>
		<Policy ruleid="57" action="1"></Policy>
		<CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
			2014-03-19T16:21:12+00:02
		</CreateTime>
		<Source>
			<Node>
				<Address ident="" category="ipv4-addr">
					<address>2.2.2.2</address>
				</Address>
			</Node>
			<Service duration="41" size="16905">
				<port>59078</port>
				<protocol>TCP</protocol>
			</Service>
		</Source>
		<Target>
			<Node>
				<Address ident="" category="ipv4-addr">
					<address>3.3.3.3</address>
				</Address>
			</Node>
			<Service duration="41" size="1448">
				<name>junos-http</name>
				<port>80</port>
				<protocol>TCP</protocol>
			</Service>
		</Target>
		<SourceNat>
			<Node>
				<name>trust</name>
				<Address category="ipv4-addr">
					<address>4.4.4.4</address>
				</Address>
			</Node>
			<Service>
				<port>59078</port>
			</Service>
		</SourceNat>
		<TargetNat>
			<Node>
				<Address category="ipv4-addr">
					<address>5.5.5.5</address>
				</Address>
			</Node>
			<Service>
				<port>80</port>
			</Service>
		</TargetNat>
	</Connect>
</SIMEF-Message>
```

Библиография

[b-ISO 8601:2004] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times.*

[b-ISO/IEC 10646] ISO/IEC 10646:2012, *Information technology – Universal Coded Character Set (UCS).*

[b-IEEE Std 1003.1] IEEE Std 1003.1-2008, *IEEE Standard for Information Technology – Portable Operating System Interface (POSIX(R)).*

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network time protocol (version 3): Specification, implementation.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP network address translator (NAT): Terminology and considerations.*

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet message format.*

[b-IETF RFC 5905] IETF RFC 5905 (2010), *Network time protocol version 4: Protocol and algorithms specification*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2016 год