

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2770

(11/2012)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА
ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Безопасность

Требования к углубленной проверке пакетов в сетях последующих поколений

Рекомендация МСЭ-Т Y.2770

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

**ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ
ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ**

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по СПП	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

**Требования к углубленной проверке пакетов в сетях
последующих поколений**

Резюме

В Рекомендации МСЭ-Т Y.2770 определяются требования к углубленной проверке пакетов (DPI) в сетях последующих поколений (СПП). В настоящей Рекомендации определяются, главным образом, требования к объектам углубленной проверки пакетов (DPI) в СПП и рассматриваются, в частности, такие аспекты, как идентификация приложений, идентификация потоков, типы проверяемого трафика, управление сигнатурами, представление отчетов системе управления сетью (NMS) и взаимодействие с функциональным объектом принятия решения в соответствии с политикой. Несмотря на то, что эти требования предназначены для СПП, они могут применяться и к другим типам сетей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2770	20.11.2012 г.	13-я

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 не получил извещения 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/>.

© ITU 2014

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
1.1 Возможность применения	1
1.2 Правила политики	2
2 Справочные документы	3
3 Определения	3
3.1 Термины, определенные в других документах.....	3
3.2 Термины, определенные в настоящей Рекомендации	4
4 Сокращение и акронимы	7
5 Условные обозначения	8
6 Требования к функциональному объекту DPI.....	9
6.1 Идентификация потока и приложения	9
6.2 Управление сигнатурами DPI	9
6.3 Аспекты проверки трафика	11
6.4 Возможность представления отчетов.....	14
6.5 Взаимодействие с функцией принятия решения в соответствии с политикой	16
6.6 Управление трафиком.....	16
6.7 Идентификация сеанса.....	17
6.8 Проверка шифрованного трафика	17
6.9 Проверка сжатого трафика	19
6.10 Обнаружение необычного трафика	19
7 Функциональные требования с точки зрения сети	19
7.1 Общие требования.....	19
7.2 Плоскости данных, управления и контроля в узле DPI.....	20
8 Интерфейсы функционального объекта DPI	22
8.1 Внешние интерфейсы DPI-FE	22
8.2 Внутренние интерфейсы DPI-FE	23
8.3 Требования к интерфейсам.....	23
9 Соображения и требования безопасности	23
9.1 Угрозы безопасности объектам DPI	23
9.2 Требования безопасности для объектов DPI	24
Приложение А – Описание дескриптора потока.....	25
А.1 Синтаксическая перспектива протокола	25
А.2 Определение значений элементов информации.....	25
А.3 Связь между дескриптором потока, идентификатором потока IPFIX и ключом потока IPFIX	26
Библиография	28

Требования к углубленной проверке пакетов в сетях последующих поколений

1 Сфера применения

В настоящей Рекомендации определяются, главным образом, требования к объектам углубленной проверки пакетов (DPI) в СПП и рассматриваются, в частности, такие аспекты, как идентификация приложений, идентификация потоков, типы проверяемого трафика, управление сигнатурами, представление отчетов системе управления сетью (NMS) и взаимодействие с функциональным объектом принятия решения в соответствии с политикой.

В настоящей Рекомендации определяются также требования к DPI трафика в неродных форматах кодирования (например, зашифрованный трафик, сжатые данные и транскодированная информация).

Любая функция DPI может быть в общих чертах описана с помощью концепции правил политики (см. пункт 1.2).

Пользователи Рекомендации и лица, использующие описанные механизмы, должны соблюдать все применимые национальные и региональные законы, нормативные акты и политические принципы. Механизм, описанный в настоящей Рекомендации МСЭ-Т, может не применяться в отношении международной корреспонденции с целью обеспечения конфиденциальности и выполнения суверенных национальных юридических требований, касающихся электросвязи, а также соблюдения Устава и Конвенции МСЭ.

В настоящей Рекомендации не рассматривается конкретное воздействие реализации функциональной возможности распределенной DPI. Требования, главным образом, касаются функциональных аспектов DPI, однако также рассматриваются и физические аспекты. В контексте сценариев преобразования функциональных аспектов в физические к сфере применения настоящей Рекомендации относится только преобразование типа один-к-одному и N-к-одному, осуществляемое между DPI-FE и DPI-PE. Другими словами, отсутствуют требования, касающиеся распределенных объектов DPI-PE.

1.1 Возможность применения

Настоящая Рекомендация применима к сценариям, указанным на рисунке 1-1:

		Тип пакетной сети	
		СПП	Сеть, не являющаяся СПП
Технология канала передачи пакетов	IP	Применима	Возможно применима
	Не относящаяся к IP	Возможно применима	Возможно применима

Y.2770(12)_F1-1

Рисунок 1-1 – Возможность применения настоящей Рекомендации

Понятие "не относящаяся к IP" относится к стекам протоколов для типов каналов передачи пакетов, не имеющих уровня протокола IP ([IETF RFC 791] и [IETF RFC 2460]).

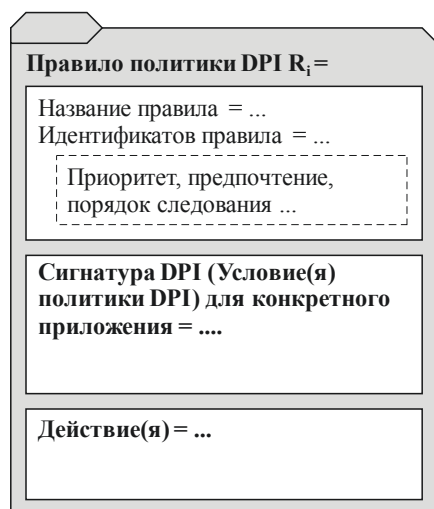
Несмотря на то, что в настоящей Рекомендации в основном рассматриваются требования к DPI в СПП, эти требования могут применяться и к другим типам сетей. Возможность их дальнейшего применения подлежит изучению.

1.2 Правила политики

В настоящей Рекомендации предусматривается применение общего высокоуровневого формата для всех правил политики. Данный высокоуровневый формат применяется к правилам DPI, как это показано на рисунке 1-2. В этом формате различаются три основных блока:

- i) идентификатор/название правила (с указанием ранга/порядка в связи с возможностью нескольких правил);
- ii) сигнатура/условия DPI;
- iii) действия.

Между действием(ями) и условием(ями) существуют логические связи, см. пункт 3.1.2.



Y.2770(12)_F1-2

Рисунок 1-2 – Общий формат правил политики DPI

Следует отметить, что в сферу применения настоящей Рекомендации входят следующие аспекты:

- описание требований, относящихся к сигнатуре DPI, (например, сигнатурам DPI, используемым для идентификации приложения и идентификации потока);
- описание требований, относящихся к идентификации и присвоению имен для правил политики DPI; и
- идентификация возможных сценариев, включающих действия в соответствии с политикой в качестве возможных последующих мер после оценки сигнатур DPI.

И наоборот, в сферу применения настоящей Рекомендации не входят следующие аспекты:

- описания требований, относящихся к действиям, которые касаются изменения проверяемого(ых) пакета(ов);
- описание явных связей между действиями и условиями (см. Примечание);
- описание правил политики DPI в полном объеме;
- описание языка для сигнатур DPI; и
- описания конкретных условий политики DPI (например, функции поведения или статистические функции).

ПРИМЕЧАНИЕ. – Например, может существовать описание действия по отбрасыванию того или иного пакета, а также условия поиска для сигнатуры пакета, однако при этом будет отсутствовать какое-либо описание, которое связывает то или иное отдельное действие с тем или иным реальным условием.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

- [ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007 г.), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS*.
- [ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic reference model: The basic model*.
- [ITU-T X.731] Recommendation ITU-T X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems management: State management function*.
- [ITU-T Y.1221] Recommendation ITU-T X.1221 (2010), *Traffic control and congestion control in IP based networks*.
- [ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in Next Generation Networks*.
- [ITU-T Y.2205] Рекомендация МСЭ-Т Y.2205 (2011 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения*.
- [ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1*.
- [ITU-T Y.2704] Рекомендация МСЭ-Т Y.2704 (2010 г.), *Механизмы и процедуры безопасности для сетей последующих поколений*.
- [IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.
- [IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6). Specification*.
- [IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 фильтр (filter) [b-IETF RFC 3198]: Набор терминов и/или критериев, используемых в целях разделения или распределения по категориям. Данная операция осуществляется с использованием сравнения заголовка трафика и/или данных полезной нагрузки по одному или нескольким полям. Регулирование и использование "фильтров" нередко осуществляется при работе сети и в политике. Например, фильтры пакетов определяют критерии сравнения с шаблоном (например, критерии протоколов IP или 802) для различения отдельных классов трафика.

ПРИМЕЧАНИЕ. – В данной Рекомендации термин "заголовок трафика" эквивалентен термину "заголовок пакета".

3.1.2 правило фильтра/политики (filter/policy rule) [b-IETF RFC 3198]: Основной структурный блок системы, основанной на политике. Представляет собой привязку набора действий к набору условий, при этом осуществляется оценка условий для определения необходимости выполнения действий.

ПРИМЕЧАНИЕ. – В данной Рекомендации правило фильтра является тем или иным конкретным правилом политики, предназначенным для разделения трафика, например, на основные категории "принятого" или "отклоненного" трафика.

3.1.3 поток (flow) [IETF RFC 5101]: Совокупность IP-пакетов, проходящих через пункт наблюдения в сети в течение определенного интервала времени. Все пакеты, принадлежащие какому-либо конкретному потоку, имеют набор общих свойств. Каждое свойство определяется как результат применения функции к значениям:

- 1) одного или нескольких полей заголовка пакета (например, IP-адрес получателя), полей заголовка транспортного уровня (например, номер порта получателя), или полей заголовка прикладного уровня (например, поле заголовка RTP [b-IETF RFC 3550]);
- 2) одной или нескольких характеристик самого пакета (например, количество меток MPLS и т. д.);
- 3) одного или нескольких полей, полученных после обработки пакета (например, следующий IP-адрес перехода по сети и выходной интерфейс).

Пакет считается принадлежащим какому-либо потоку, если он полностью удовлетворяет всем определенным свойствам этого потока.

Данное определение охватывает широкий выбор потоков – от потока, который содержит все пакеты, наблюдаемые на сетевом интерфейсе, до потока, содержащего всего один пакет между двумя приложениями. Сюда относятся пакеты, отобранные с помощью механизма составления выборки.

ПРИМЕЧАНИЕ. – В приведенных выше элементах нумерованного списка указаны свойства потока в следующих категориях: 1) "управляющая информация протокола (PCI), относящаяся к пакетам"; 2) "свойства пакетов, относящиеся к протокольному блоку данных (PDU)"; и 3) "локальная информация о передаче пакетов".

3.1.4 политика (policy) [b-IETF RFC 3198]: Набор правил по руководству и управлению доступом к ресурсам сети, а также контролю этого доступа.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 приложение (application): Обозначает одно из следующих понятий:

- *тип протокола приложения* (например, протоколы IP-приложения, видео МСЭ-Т H.264 или протокол инициирования сеанса связи (SIP));
- *экземпляр обслуживаемого пользователя* (например, VoIP, VoLTE, VoIMS, VoNGN, и VoP2P), относящегося к типу приложения, например, "приложения по передаче голоса в пакетном режиме";
- *"приложение, определяемое поставщиком"*, предназначенное для передачи голоса в пакетном режиме (например, VoIP поставщика SGPP, Skype VoIP);
- приложение, вложенное в другое приложение (например, контент приложения в элементе тела сообщения SIP или HTTP).

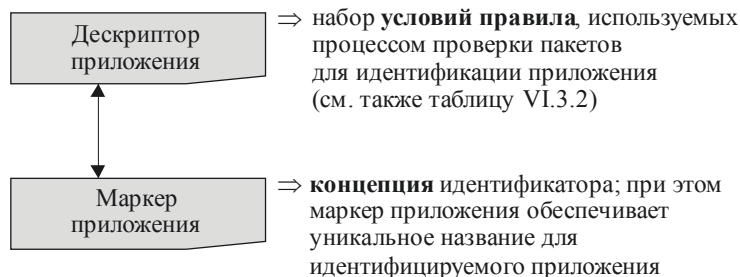
Приложение может быть определено с помощью конкретного идентификатора (например, посредством битового поля, шаблона, сигнатуры или регулярного выражения в качестве "условий прикладного уровня", см. также пункт 3.2.2), в виде общих характеристик всех перечисленных выше уровней приложений.

3.2.2 дескриптор приложения (application-descriptor) (также называемый условиями прикладного уровня (application-level conditions)): Набор условий правила, который идентифицирует приложение (в соответствии с пунктом 3.2.1).

В настоящей Рекомендации рассматривается дескриптор приложения как объект в целом, который является синонимом условий прикладного уровня. В Рекомендации не рассматривается подробная структура дескриптора, например синтаксис, кодирование и тип данных.

3.2.3 маркер приложения (application tag): Уникальное название приложения, которое используется для обозначения семантики приложения и обычно используется в сценариях представления отчетов.

На рисунке 3-1 изображена взаимосвязь между маркером приложения и дескриптором приложения.



Y.2770(12)_F3-1

Рисунок 3-1 – Взаимосвязь маркера приложения и дескриптора приложения

3.2.4 двунаправленная DPI (bidirectional DPI): DPI, которая включает условия политики, касающиеся обоих направлений трафика.

ПРИМЕЧАНИЕ. – В случае двунаправленной DPI существует по меньшей мере по одному простому условию на направление трафика.

3.2.5 углубленная проверка пакетов (deep packet inspection (DPI)): Проведение в соответствии с базовой эталонной моделью взаимодействия открытых систем (OSI-BRM) [ITU-T X.200], предусматривающей уровневую архитектуру протокола, анализа:

- свойств полезной нагрузки и/или пакетов (см. в пункте 3.2.11 список возможных свойств), более полных, чем информация заголовка на уровнях 2, 3 и 4 (L2/L3/L4) протокола; и
- других свойств пакета

в целях однозначного определения приложения.

ПРИМЕЧАНИЕ. – Результат применения функции DPI, наряду с некоторой дополнительной информацией, например, информацией о потоке, как правило, используется в последующих функциях, таких как представление отчета, или в действиях в отношении пакета.

3.2.6 ядро DPI (DPI engine): Подкомпонент и главная часть функционального объекта DPI, которая выполняет все функции обработки в тракте передачи пакета (например, идентификацию пакета и другие функции обработки пакета, изображенные на рисунке 6-1).

3.2.7 объект DPI (DPI entity): Объектом DPI является либо функциональный объект DPI, либо физический объект DPI.

3.2.8 функциональный объект DPI (DPI functional entity (DPI-FE)): Функциональный объект, который выполняет углубленную проверку пакетов.

3.2.9 физический объект DPI (DPI physical entity (DPI-PE)): Реализованный экземпляр функционального объекта DPI.

3.2.10 политика DPI (DPI policy): Политика, определенная, например, в [b-IETF RFC 3198] (см. пункт 3.1.4), которая осуществляется в объекте DPI.

3.2.11 условие политики DPI (DPI policy condition) (также называемое сигнатурой DPI (DPI signature)): Представление необходимых состояния и/или предварительных условий, по которым идентифицируется приложение и определяется необходимость выполнения действий, предусмотренное правилом политики. Набор условий политики DPI, связанных с каким-либо правилом политики, определяет случаи применения этого правила политики (см. также [b-IETF RFC 3198]).

Условие политики DPI должно содержать условия прикладного уровня и может содержать другие варианты, например условия состояния и/или условия уровня потока:

- 1) условие состояния (факультативно):
 - a) условия категории обслуживания сетью (например, наличие перегрузки в трактах передачи пакетов); или
 - b) статус элементов сети (например, локальное условие переполнения DPI-FE).
- 2) дескриптор потока / условия уровня потока (факультативно):
 - a) содержимое пакета (поля заголовка);
 - b) характеристики пакета (например, число меток MPLS);
 - c) обработка пакета (например, выходной интерфейс DPI-FE);
- 3) дескриптор приложения / условия прикладного уровня:
 - a) содержимое пакета (поля заголовка приложения и полезная нагрузка приложения).

ПРИМЕЧАНИЕ. – Это условие относится к "простому условию" в формальных описаниях условий уровня потока и условий прикладного уровня.

3.2.12 функциональный объект принятия решения в соответствии с политикой DPI (DPI policy decision functional entity (DPI-PDFE)): Удаленная функция по отношению к DPI-FE, которая принимает решение о реализации в DPI-FE правил, основанных на сигнатуре. Некоторые функции контроля и/или управления не всегда могут быть удаленными по отношению к DPI-FE.

3.2.13 правило политики DPI (DPI policy rule): Правило политики, относящееся к DPI (см. также пункт 3.1.2). В настоящей Рекомендации правило политики DPI называется просто правилом.

3.2.14 сигнатура DPI (DPI signature): Синоним условия(й) политики DPI (см. пункт 3.2.11).

3.2.15 библиотека сигнатур DPI (DPI signature library): База данных, состоящая из набора сигнатур DPI, которая называется также библиотекой протокола DPI, потому что сигнатуры, как правило, могут использоваться для идентификации протокола.

3.2.16 дескриптор потока (flow descriptor) (также называемый условиями уровня (level conditions)): Набор условий правила, которые используются для идентификации конкретного типа потока (в соответствии с пунктом 3.1.3) в проверяемом трафике.

ПРИМЕЧАНИЕ 1. – Настоящее определение дескриптора потока расширяет определение, приведенное в [b-ITU-T Y.2121], за счет дополнительных элементов, описанных в пункте 3.

ПРИМЕЧАНИЕ 2. – Дополнительное обсуждение нормативных аспектов дескриптора потока, используемого в настоящей Рекомендации, приведено в Приложении А.

3.2.17 идентификатор потока IPFIX (IPFIX flow identifier (IPFIX flow ID)): Набор значений ключей потока IPFIX, которые используются в сочетании с дескриптором потока для идентификации того или иного конкретного потока.

3.2.18 ключ потока IPFIX (IPFIX flow key): Каждый из элементов информации дескриптора потока, который используется в процессах идентификации потока на основе IPFIX (в соответствии с [IETF RFC 5101]).

ПРИМЕЧАНИЕ. – Определение ключа потока IPFIX семантически согласуется с определением ключа потока, приведенным в IPFIX [IETF RFC 5101]. Единственное отличие между этими двумя терминами заключается в том, что в настоящем документе определение ограничено дескриптором потока.

3.2.19 проверка заголовков L3,4 (L3,4 Header Inspection (L_{3,4}HI)): Выполнение правила (правил) политики и условий политики, затрагивающее только элементы управляющей информации протокола (PCI) сетевого уровня или/и транспортного уровня.

3.2.20 проверка заголовков L4+ (L4+ Header Inspection (L₄₊HI)): Выполнение правила (правил) политики и условий политики, затрагивающее только элементы PCI, расположенные выше транспортного уровня.

3.2.21 проверка полезной нагрузки L4 (L4 Payload Inspection (L₄PI)): Выполнение правила (правил) политики и условий политики, затрагивающее только полезную нагрузку транспортного уровня, которой могут являться "данные приложения", предназначенные для конкретных прикладных протоколов (например, SIP).

ПРИМЕЧАНИЕ. – L₄PI относится к объединению условий политики L₄₊HI и L₇PI.

3.2.22 проверка полезной нагрузки L7 (L7 Payload Inspection (L7PI)): Выполнение правила (правил) политики и условий политики на основе данных приложения.

3.2.23 полезная нагрузка (payload): Блок данных, следующих в пакете за элементами заголовка, за исключением дополнительных элементов, расположенных в конце пакета (например, элементов заполнителя, трейлера и контрольной суммы).

ПРИМЕЧАНИЕ 1. – Таким образом, понятие полезной нагрузки является синонимом блока служебных данных (SDU) в OSI-BRM [ITU-T X.200], понятие пакета – синонимом протокольного блока данных (PDU), а понятие управляющей информации протокола (PCI) охватывает все элементы заголовка и трейлера пакета. Таким образом, "PDU = PCI + SDU".

ПРИМЕЧАНИЕ 2. – Понятие полезной нагрузки относится к конкретному уровню протокола (т. е. *полезная нагрузка Lx* означает полезную нагрузку на уровне x протокола). То же самое относится к *Lx-SDU*, *Lx-PDU* и *Lx-PCI*.

4 Сокращение и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

АН	Authentication Header	Заголовок аутентификации
BRM	Basic Reference Model	Базовая эталонная модель
DCCP	Datagram Congestion Control Protocol	Протокол контроля перегрузок для дейтаграмм
DPI	Deep Packet Inspection	Углубленная проверка пакета
DPI-FE	DPI Functional Entity	Функциональный объект DPI
DPI-PDFE	DPI Policy Decision Functional Entity	Функциональный объект принятия решения в соответствии с политикой DPI
DPI-PE	DPI Physical Entity	Физический объект DPI
DPI-PIB	DPI Policy Information Base	База информации о политике DPI
ESP	Encapsulating Security Payload	Инкапсуляция полезной нагрузки безопасности
ET	Emergency Telecommunications	Электросвязь в чрезвычайных ситуациях
FPA	Full Payload area Analysis	Полный анализ области полезной нагрузки
FSL	Filter Specification Language	Язык описания фильтров
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
IANA	Internet Assigned Numbers Authority	Орган присвоения номеров интернета
IE	Information Elements	Элементы информации
IP	Internet Protocol	Протокол Интернет
IPFIX	IP Flow Information Export	Экспорт информации о потоке IP
IS	In-Service	В рабочем состоянии
L-PDF	Local PDF	Локальная PDF
MPLS	Multi Protocol Label Switching	многопротокольная коммутация с использованием меток
NGN	Next Generation Network	СПП Сеть последующих поколений
NMS	Network Management System	Система управления сетью
OGP	Open Game Protocol	Открытый протокол игр
OoS	Out-of-Service	В нерабочем состоянии
OSI-BRM	Open Systems Interconnection – Basic Reference Model	Взаимосвязь открытых систем – Базовая эталонная модель

P2P	Peer to Peer	Одноранговый
PCC	Policy and Charging Control	Управление политикой и начислением платы
PCI	Protocol Control Information	Управляющая информация протокола
PDF	Policy Decision Function	Функция принятия решения в соответствии с политикой
PDU	Protocol Data Unit	Протокольный блок данных
PEL	Policy Expression Language	Язык выражения политики
PFF	Packet Forwarding Function	Функция пересылки пакетов
PIB	Policy Information Base	База информации о политике
PPA	Payload area Analysis	Анализ области полезной нагрузки
PSAMP	Packet Sampling	Составление выборки пакетов
PSL	Policy Specification Language	Язык описания политики
RACF	Resource and Admission Control Functions	Функции управления ресурсами и допуском
RACS	Resource and Admission Control Subsystem	Подсистема управления ресурсами и допуском
R-PDF	Remote PDF (i.e., PDF remotely located from DPI node perspective)	Удаленная PDF (т. е. PDF, находящаяся на расстоянии с точки зрения узла DPI)
RTP	Real-time Transport Protocol	Протокол транспортирования в реальном времени
SA	Security Association (IPsec)	Ассоциация безопасности (IPsec)
SCTP	Stream Control Transmission Protocol	Протокол передачи для управления потоком
SDU	Service Data Unit	Блок служебных данных
SigComp	Signaling Compression	Сжатие сигнала
SIP	Session Initiation Protocol	Протокол инициирования сеанса связи
SPI	Security Parameter Index (IPsec)	Индекс параметров безопасности (IPsec)
TCP	Transmission Control Protocol	Протокол управления передачей
TISPAN	Telecommunication and Internet Converged Services and Protocols for Advanced Networking	Конвергированные услуги и протоколы электросвязи и интернета для усовершенствованных сетей
UDP	User Datagram Protocol	Протокол дейтаграммы пользователя

5 Условные обозначения

В настоящем документе содержится список элементов, обозначенных как *R-x/y*, где *x* обозначает номер пункта, а *y* – номер в рамках этого пункта. В таких элементах используются следующие ключевые слова, значения которых установлены ниже:

Ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "запрещается" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "рекомендуется, чтобы" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии этому документу это требование не является обязательным.

Ключевые слова "может факультативно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии спецификации.

В тексте настоящей Рекомендации и его дополнениях иногда встречаются слова "должен", "не должен", "следует" и "может". В этом случае их следует понимать как "требуется, чтобы", "запрещено", "рекомендуется" и "может факультативно", соответственно. Появление таких фраз или ключевых слов в дополнении или материалах, однозначно помеченных, как информативных, должно пониматься, как не несущее нормативного смысла.

6 Требования к функциональному объекту DPI

6.1 Идентификация потока и приложения

R-6.1/1: Требуется, чтобы функциональный объект DPI выполнял идентификацию приложения.

R-6.1/2: Требуется, чтобы функциональный объект DPI поддерживал различные виды правил политики DPI.

R-6.1/3: Требуется, чтобы DPI-FE идентифицировал какое-либо приложение путем проверки его полезной нагрузки.

R-6.1/4: Требуется, чтобы условия прикладного уровня (и дополнительные условия уровня потока) позволяли идентифицировать приложение на основе однонаправленного трафика (однаправленная DPI) для всех однонаправленных приложений и для двунаправленных приложений при условии, что одно направление трафика обеспечивает возможность однозначной идентификации.

R-6.1/5: Требуется, чтобы условия прикладного уровня (и дополнительные условия уровня потока) могли факультативно позволить идентифицировать приложение на основе двунаправленного трафика (двунаправленная DPI).

R-6.1/6: Рекомендуется, чтобы элементы информации, используемые в условиях уровня потока, соответствовали [b-IETF RFC 5102], как это зарегистрировано в IANA [b-IETF IANA IPFIX]. В таком случае рекомендуется, чтобы элементы информации включали элементы информации IPFIX, относящиеся к канальному (L2), сетевому (L3) и транспортному (L4) уровням протокола, которые соответствуют базовой уровневой архитектуре протокола IETF.

ПРИМЕЧАНИЕ. – Реестр IANA, предназначенный для элементов информации IPFIX, может быть факультативно расширен путем включения (со стороны IETF) дополнительных элементов. В существующем реестре IANA (по состоянию на конец 2011 г.) отсутствуют элементы информации для уровней L4 протоколов, отличных от протоколов UDP и TCP (например, для SCTP и DCCP).

R-6.1/7: Элементы информации могут факультативно являться другими элементами информации, относящимися к уровням L2, L3 или L4 и не входящими в реестр IPFIX (в протоколе IPFIX [IETF RFC 5101] они называются элементами информации, определяемыми предприятием).

6.2 Управление сигнатурами DPI

В данном пункте определяются требования, касающиеся операций в отношении библиотеки сигнатур DPI. Такие операции могут быть локально инициированы DPI-FE или инициированы удаленным объектом сети (см. рисунок 6-1). Все возможные типы удаленных объектов сети могут рассматриваться в качестве функционального объекта принятия решения в соответствии с политикой, который принимает решение о реализации в DPI-FE правил, основанных на сигнатуре.



Рисунок 6-1 – Управление сигнатурами DPI в контексте примера архитектуры функционального объекта DPI (см. также рисунок 8-2, в том что касается внутренних интерфейсов)

Функциональный объект принятия решения в соответствии с политикой DPI должен быть связан с RACF (в случае СПП, имеющей RACF), однако его описание не входит в сферу применения настоящей Рекомендации. На рисунке 6-1 он указан потому, что содержит удаленные функции управления DPI-FE.

6.2.1 Общие требования к сигнатурам

R-6.2.1/1: Требуется, чтобы сигнатуры DPI хранились в *библиотеке сигнатур DPI*, которая является подобъектом DPI-FE.

ПРИМЕЧАНИЕ. – Основная причина использования локальной библиотеки сигнатур DPI заключается в том, что функции идентификации пакета требуется незамедлительный доступ к содержимому этой базы данных.

Сигнатура DPI может использоваться для:

- примерной идентификации (например, поведение, эвристика и т. д.); и
- точной идентификации (например, точные правила соответствия).

Язык (формальный или поведенческий), используемый для определения правил политики в настоящей библиотеке, а также сами правила соответствия не входят в сферу применения настоящей Рекомендации. В ней определяется только факт существования библиотеки сигнатур DPI, суть сигнатур DPI, а также функции управления библиотекой.

R-6.2.1/2: Требуется, чтобы библиотека сигнатур DPI велась с соблюдением мер безопасности и была невидима для несанкционированных пользователей.

6.2.2 Управление библиотекой сигнатур DPI

В данном пункте определяются требования к управлению библиотекой сигнатур DPI.

6.2.2.1 Добавление новых сигнатур

R-6.2.2.1/1: Требуется, чтобы в библиотеку сигнатур DPI можно было добавлять новые сигнатуры DPI.

6.2.2.2 Операции над существующими сигнатурами

R-6.2.2.2/1: Требуется, чтобы можно было изменять (обновлять) существующие сигнатуры в библиотеке сигнатур DPI.

R-6.2.2.2/2: Требуется, чтобы можно было подключать и отключать конкретные сигнатуры DPI в библиотеке сигнатур DPI.

R-6.2.2.2/3: Требуется, чтобы можно было исключать (удалять) конкретные сигнатуры DPI в библиотеке сигнатур DPI.

6.2.2.3 Формат правила, обмен которым осуществляется по внешнему интерфейсу

R-6.2.2.3/1: Сигнатура DPI для идентификации приложения, обмен которой осуществляется по внешним интерфейсам (например, *e1* и *e2* на рисунке 8-1), может факультативно соответствовать любому формату правила (см. также пункт 1.2).

6.2.3 Расположение функции управления

R-6.2.3/1: Требуется, чтобы действия в рамках управления сигнатурами DPI, определенные в пункте 6.2.2, осуществлялись из функционального объекта DPI либо локально, либо дистанционно, либо обоими способами (см. рисунок 6-1).

6.2.4 Инициирование управляющих действий

R-6.2.4/1: Требуется, чтобы в отношении операций над сигнатурами DPI поддерживался принудительный ("push") режим, в случае если эти операции иницируются дистанционно (например, со стороны DPI-PDFE на рисунке 6-1).

R-6.2.4/2: Требуется, чтобы в отношении операций над сигнатурами DPI поддерживался опросный ("pull") режим, в случае если эти операции иницируются DPI-FE локально. Понятие "опросный" означает, что локальная функция управления DPI-FE направляет запрос DPI-PDFE на осуществление управляющего действия в отношении новой или существующей сигнатуры.

Способы инициирования запроса DPI-FE не входят в сферу применения настоящей Рекомендации.

6.3 Аспекты проверки трафика

В данном пункте рассматриваются аспекты, касающиеся типов трафика, к которому применяется DPI.

6.3.1 Аспекты идентификации потока

R-6.3.1/1: Рекомендуются, чтобы функциональный объект DPI поддерживал идентификацию приложений без осуществления проверки на уровне потока (см. также рисунок VII-7).

R-6.3.1/2: Любой сценарий DPI первоначально может быть факультативно независимым от потока, т. е. в предоставляемом DPI-FE правиле политики DPI не должен содержаться дескриптор потока. Однако это правило может направить запрос о сборе интересующей информации о потоке.

R-6.3.1/3: Требуется, чтобы в таком запросе был предоставлен какой-либо ключ потока IPFIX, а также факультативно заполнена недостающая информация о потоке.

R-6.3.1/4: Функциональный объект DPI может факультативно потребовать полного распознавания идентификатора потока IPFIX на основе заданного ключа потока IPFIX и проверки нескольких последовательных пакетов.

R-6.3.1/5: Действие полного или неполного идентификатора потока IPFIX по представлению DPI-FE отчета удаленному объекту сети может факультативно определяться условием (например, предопределяться событием, управляться таймером и т. д.).

6.3.2 Аспекты DPI при наличии и отсутствии информации о стеке протоколов

Функция идентификации DPI (в рамках DPI-FE) отвечает за идентификацию приложения и касается операций сравнения и поиска на основе сигнатуры DPI, осуществляемых в отношении входящего пакета (PDU). Существует два варианта: DPI-FE либо имеет информацию о внутренней структуре PDU (т. е. "DPI-FE, имеющий информацию о стеке протоколов"), либо не имеет информации его структуры ("DPI-FE, не имеющий информации о стеке протоколов").

Оба варианта могут обеспечить одинаковый результат идентификации и быть функционально эквивалентными. Основное отличие состоит в том, что логика идентификации при наличии информации о стеке протоколов, возможно, является более эффективной.

В том что касается операционной эффективности (т. е. идентификации приложения и факультативной идентификации потока) целесообразно различать следующие два вида анализа:

- a) анализ предварительно определенной области полезной нагрузки (PPA): когда пакеты (поток) соответствуют известному приложению с четко определенной структурой полезной нагрузки, DPI-FE может проверять предварительно определенное фиксированное место в полезной нагрузке (т. е. режим проверки пакетов при наличии информации о стеке протоколов);
- b) анализ полной области полезной нагрузки (FPA): когда пакеты (поток) не соответствуют какому-либо известному приложению, или структура полезной нагрузки приложения четко не определена или не известна, DPI-FE проверяет "область полезной нагрузки" целиком (т. е. режим проверки пакетов при отсутствии информации о стеке протоколов).

Как PPA, так и FPA могут применяться к одному и тому же потоку трафика.

R-6.3.2/1: Рекомендуются, чтобы DPI-FE поддерживал идентификацию приложений при наличии информации о стеке протоколов.

R-6.3.2/2: Рекомендуются, чтобы DPI-FE поддерживал идентификацию приложений, при отсутствии информации о стеке протоколов.

R-6.3.2/3: Требуется, чтобы DPI-FE идентифицировал приложения, владея информацией о стеке протоколов IPv4 и IPv6, и мог дополнительно идентифицировать приложения, владея информацией о другом основном стеке протоколов.

R-6.3.2/4: Рекомендуются, чтобы DPI-FE идентифицировал приложения во вложенном трафике, например, в инкапсулированном или туннелированном трафике.

6.3.3 Аспекты, связанные с действиями в соответствии с правилами политики DPI

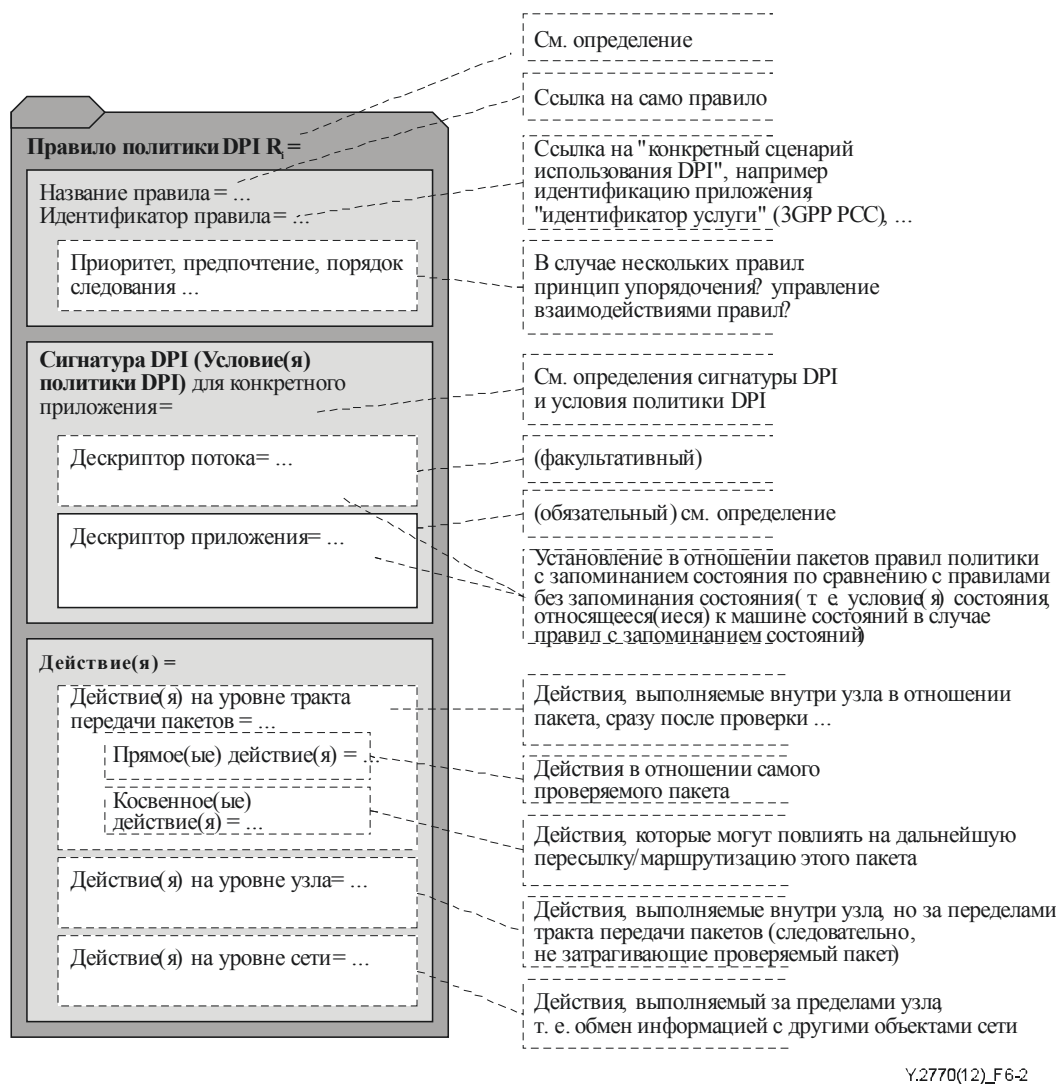
6.3.3.1 Базовая информация

Действия в соответствии с политикой DPI могут выполняться на разных иерархических уровнях, например, DPI-FE, локальной PDF и удаленной PDF. Эти действия могут включать, например, следующее.

- 1) Действия на уровне тракта передачи пакетов (со стороны DPI-FE):
 - a) принятие пакета и его пересылка функции пересылки пакетов (PFF) (действие по условию, только для режима "DPI в тракте");
 - b) отбрасывание пакета (без объявления или иным образом);
 - c) перенаправление пакета другим выходным интерфейсам;
 - d) копирование/дублирование пакета для других выходных интерфейсов;
 - e) классификация трафика, локальные изменения и представление отчета о данных изменений;
 - f) методы установления приоритета, блокирования, формирования и распределения применительно к отдельным пакетам.
- 2) Действия на уровне узла (с использованием "локальной функции принятия решения в соответствии с политикой" (L-PDF)):
 - a) динамическое создание новых правил политики DPI и/или изменение существующих правил (хранящихся в базе данных информации о политике DPI (DPI-PIB));
 - b) создание данных по регистрации/отслеживанию и представление отчета функции управления политикой (см. пункт 2.11.2 в [b-IETF RFC 3871]);
 - c) обнаружение и представление отчета о неидентифицируемых приложениях;
 - d) уведомление систем обнаружения проникновений (например, путем предоставления образцов трафика, подозрительных пакетов).

- 3) Действия на уровне сети (посредством "удаленной функции принятия решения в соответствии с политикой" (R-PDF)):
- a) управление ресурсами, контроль допуска и высокоуровневая фильтрация (на уровне подсистем сети (определенных, например, для RACF в [ITU-T Y.2111], ETSI TISPA RACS [b-ETSI ES 282 003] и 3GPP PCC [b-ETSI TS 123 203]);
 - b) начисление платы за контент на основе типов приложений абонента (например, RADIUS или Diameter IETF).

На рисунке 6.2 дополнительно разъясняются указанные выше структурные принципы с помощью подробного обобщенного формата правила политики (по сравнению с форматом, представленным в пункте 1.2):



Пример 6-2 – Пример подробного формата правила политики (по сравнению с рисунком 1-2)

Сопоставление конкретных действий и условий не входит в сферу применения настоящей Рекомендации.

6.3.3.2 Требования

R-6.3.3.2/1: После того, как приложение было идентифицировано DPI-FE, может быть факультативно обеспечена возможность извлечения информации, относящейся к приложению.

Например, URL в HTTP, формат носителя ("тип кодака") в протоколе транспортирования в реальном времени (RTP), или идентификатор сеанса RTP (например, SSRC для окончного пункта источника RTP).

R-6.3.3.2/2: DPI-FE может факультативно обеспечивать возможность совместной работы с функцией измерения потока, например, процессом изменения IPFIX [IETF RFC 5101] и рядом функций фильтрации, таких как в [b-IETF RFC 5476].

ПРИМЕЧАНИЕ. – Как правило, в процессе измерения заполняются следующие элементы информации IPFIX (используемые как ключи потока): sourceIPv6Address и destinationIPv6Address, sourceIPv4Address и destinationIPv4Address, protocolIdentifier, sourceTransportPort, destinationTransportPort и т. д. Однако роль DPI-FE состоит в том, чтобы заполнить маркер приложения и идентификатор потока IPFIX (на основе данного ключа потока IPFIX, см. также рисунок A.1).

6.4 Возможность представления отчетов

Представление отчета касается уведомления (например, в связи с обнаружением DPI-FE какого-либо конкретного события) другого функционального объекта, который, как правило, находится в удаленном элементе сети (в плоскости пользователя, контроля или управления). DPI-FE может обеспечивать несколько интерфейсов для представления отчетов, поддерживающих "различные типы событий".

6.4.1 Представление отчета системе управления сетью (NMS)

6.4.1.1 Интерфейс и протокол для представления отчетов

R-6.4.1.1/1: Рекомендуются, чтобы протокол экспорта соответствовал спецификации IPFIX [IETF RFC 5101]. Он может факультативно соответствовать расширениям IPFIX.

R-6.4.1.1/2: В случае двунаправленных потоков протокол экспорта может факультативно соответствовать спецификации IPFIX [b-IETF RFC 5103].

R-6.4.1.1/3: Рекомендуются, чтобы в протоколах экспорта, базирующихся на IPFIX, использовался внешний интерфейс e2 (см. рисунок 8-1).

6.4.1.2 Информация, представляемая в отчете

R-6.4.1.2/1: Требуется, чтобы DPI-FE представлял плоскости управления DPI информацию о результатах проверки (например, маркер приложения и, теоретически, элементы информации, относящиеся к приложению), а также информацию, относящуюся к потоку. Локально обновляемые значения ключа потока (включая типовые поля функции измерения потока) могут быть факультативно экспортированы в функцию принятия решения в соответствии с политикой (например, PD-FE, определенному в [ITU-T Y.2111]).

R-6.4.1.2/2: Рекомендуются, чтобы в представляемой в отчете информации повторно использовались элементы информации IPFIX ([b-IETF IANA IPFIX]), которые были первоначально определены в информационной модели IPFIX [b-IETF RFC 5102].

Информация, относящаяся к потоку, определена в информационной модели IPFIX [b-IETF RFC 5102], например:

- 1) информация, относящаяся к приложению:
 - маркер приложения; и
 - извлеченные поля, например, медиаформат RTP и SSRC RTP;
- 2) поля заголовков L3/L4, соответствующие адресам IP, порты L4 (например, TCP или UDP, см. Примечание 1) и тип протокола;
- 3) информация о показателях работы (например, метрика, статистические данные) число байтов, число пакетов и максимальный размер пакета (см. Примечание 2);
- 4) информация о времени: время начала потока, время окончания потока;
- 5) информация, относящаяся к пакету: следующий переход по сети и размер пакета (см. Примечание 3).

ПРИМЕЧАНИЕ 1. – Некоторые из перечисленных элементов (еще) не входят в реестр IPFIX Органа присвоения номеров интернета (IANA), однако они являются действительными в контексте настоящей Рекомендации.

ПРИМЕЧАНИЕ 2. – Информация, относящаяся к потоку, может создаваться механизмом составления выборки пакетов (PSAMP), однако при экспортировании таких результатов в NMS рекомендуется добавлять информацию, относящуюся к приложению.

ПРИМЕЧАНИЕ 3. – Возможно, придется зарегистрировать некоторые новые элементы информации в IPIX IANA, в соответствии с разделом 7 "IANA Considerations" [b-IETF RFC 5102].

6.4.2 Представление информации о новом, неизвестном или неправильном приложении

6.4.2.1 Характеристики такого трафика

Между этими видами приложений существуют незначительные различия. Для этих приложений могут быть характерны следующие конкретные свойства, что приводит к использованию различных условий прикладного уровня для их обнаружения:

- новое приложение: например, новая версия приложения, новая версия элемента информации, относящегося к приложению (например, новая версия игры в рамках открытого протокола игр (OGP)) или новая версия протокола; можно отметить, что понятие "новый" отражает перспективу услуги DPI (которая может базироваться на хронологической последовательности прежних услуг DPI);
- неизвестное приложение: например, неизвестный тип пакета, неизвестный протокол, неизвестное "приложение";
- неправильное приложение: например, пакет, содержащий неправильную грамматику протокола (см. Примечание), и т. д.

ПРИМЕЧАНИЕ. – Неправильный синтаксис протокола может быть использован для атаки, нарушающей безопасность. Как правило, затронутыми оказываются те протоколы, которые завершаются в оборудовании пользователя (например, протоколы сигнализации).

6.4.2.2 Требования к представлению отчетов

R-6.4.2.2/1: DPI-FE может факультативно обеспечивать представление отчетов о новых, неизвестных или неправильных приложениях по результатам проверки трафика.

6.4.3 Представление отчетов о необычном трафике

R-6.4.3/1: DPI-FE может факультативно обеспечивать возможность представления отчетов об обнаружении необычного трафика после обнаружения такого трафика.

Согласно определению, необычный трафик – это трафик, не относящийся к классам обычного трафика. Класс обычного трафика представляет собой совокупность видов трафика, которые соответствуют существующим статистическим свойствам строго определенных приложений, таким как разница во времени прихода последовательных пакетов, порядок прихода пакетов, размер PDU конкретного уровня протокола, размер полезной нагрузки или объем трафика (на каком-либо конкретном уровне протокола).

6.4.4 Представление отчетов о событиях, относящихся к DPI-PE

В данном пункте описываются события, касающиеся операционного состояния объекта DPI, а также соответствующие требования к представлению отчетов.

6.4.4.1 Случаи отказов, относящиеся к неправильному поведению DPI-PE

Простейшим способом описания управляющего состояния DPI-PE является описание с точки зрения двух состояний: "в рабочем состоянии" (IS) и "в нерабочем состоянии" (OoS).

R-6.4.4.1/1: Рекомендуется, чтобы управление DPI базировалось на современном состоянии (например, [ITU-T X.731] и [b-IETF RFC 4268]) и поддерживало по меньшей мере управляющие состояния, соответствующие IS и OoS.

R-6.4.4.1/2: При любом отказе DPI-PE, если его резервирование не предусмотрено архитектурой, может факультативно осуществляться переход из состояния IS в состояние OoS. Рекомендуется представлять отчет о таких событиях.

6.4.4.2 События, относящиеся к управлению устранением неисправностей DPI-PE

DPI-PE обеспечивает сетевые интерфейсы для входящего и исходящего трафика, на которых могут возникать неисправности.

R-6.4.4.2/1: Рекомендуется, чтобы DPI-PE поддерживал функцию аварийного оповещения, как это определено в [b-ITU-T X.734].

6.4.4.3 События, относящиеся ко входу в систему функционального объекта DPI

R-6.4.4.3/1: Функциональный объект DPI может факультативно обеспечивать возможность входа в систему в соответствии, например, с Syslog [b-IETF RFC 5424]. В таких случаях функциональный объект DPI является исходящим пунктом сообщений Syslog.

Следует отметить, что в случае, когда в проверяемом потоке пакетов передается трафик сообщений входа в систему, функциональный объект не является ни исходящим, ни конечным пунктом сообщений входа в систему. Другими словами, ключ для просмотра такого потока пакетов может основываться на дескрипторе приложения (относящемся к прикладному уровню syslog) и на дескрипторе потока IPFIX (относящемся к выбранному транспортному режиму syslog). Дополнительная информация представлена в [b-IETF RFC 5424] и [b-IETF RFC 5426].

6.4.4.4 События, относящиеся к состоянию загрузки физического объекта DPI и потреблению им ресурсов

DPI-PE имеет ограниченные ресурсы для обработки DPI. Конкретные данные о ресурсах зависят от реализации и не входят в сферу применения настоящей Рекомендации.

R-6.4.4.4/1: Рекомендуется, чтобы физический объект DPI обеспечивал представление плоскости управления отчета об уровне загрузки ресурсных компонентов DPI.

Например, в сетях, передающих трафик электросвязи в чрезвычайных ситуациях (см. пункт 7.1.1), процесс DPI должен иметь возможность передачи этого трафика через сильно загруженные узлы сети; в связи с этим целесообразно, чтобы система управления сетью была информирована об уровне загрузки.

6.5 Взаимодействие с функцией принятия решения в соответствии с политикой

R-6.5/1: DPI-FE может факультативно действовать в рамках функционального объекта реализации политики, определенного в [ITU-T Y.2111], и обеспечивать соответствующую функцию транспортирования.

R-6.5/2: Интерфейсом между DPI-FE и RACF факультативно может являться интерфейс *Rw*, определенный в [ITU-T Y.2111].

R-6.5/3: Обмен информацией между DPI-FE и RACF PD-FE может факультативно осуществляться через существующий интерфейс (например, *Rw*) или новый интерфейс RACF, в зависимости от конкретного сценария использования DPI.

ПРИМЕЧАНИЕ. – В этом случае RACF должна быть расширена и включать информацию DPI (например, сигнатуру протокола в правиле политики DPI); RACF, определенная в [ITU-T Y.2111], поддерживает, в первую очередь, правила политики, основанные на идентификации потока. Конкретная эталонная точка RACF будет зависеть от конкретного сценария использования DPI.

6.6 Управление трафиком

Можно сформулировать следующие высокоуровневые требования:

R-6.6/1: Функциональный объект DPI может быть факультативно задействован в сетевых сценариях в целях управления трафиком (например, функциях управления трафиком, определенных в [ITU-T Y.1221]). Рекомендуется, чтобы DPI-FE поддерживал соответствующие возможности управления трафиком.

R-6.6/2: DPI-FE может факультативно поддерживать управление трафиком по умолчанию. Тем не менее подробные функциональные требования к управлению трафиком не входят в сферу применения настоящей Рекомендации.

R-6.6/3: DPI-FE может факультативно поддерживать взаимодействие с внешними функциями управления трафиком. Относящиеся к этим функциям требования не входят в сферу применения настоящей Рекомендации.

6.7 Идентификация сеанса

В настоящей Рекомендации имеется много терминов, относящихся к сеансу. DPI-FE может однозначно идентифицировать весь трафик какого-либо сеанса, поскольку "дескриптор сеанса" либо равен поднабору дескриптора потока и/или приложения, либо является им.

6.7.1 Требования к идентификации сеанса

R-6.7.1/1: Требуется, чтобы DPI-FE мог анализировать режим сеанса (например, сеанса RTP, сеанса HTTP, сеанса IM, сеанса VoIP SIP).

R-6.7.1/2: Требуется, чтобы DPI-FE мог отслеживать состояние сеанса.

6.7.2 Действия DPI на "уровне сеанса"

R-6.7.2/1: DPI-FE может факультативно извлекать или создавать данные измерений на уровне сеанса (например, для контроля показателей работы, относящихся к оценке пользователем качества услуги).

6.8 Проверка шифрованного трафика

Существует единое мнение, что сигнатуры DPI могут применяться только к нешифрованному трафику. Тем не менее сигнатуры DPI могли бы применяться к шифрованному трафику, в зависимости от:

- уровня шифрования (см. пункт 6.8.1);
- локального наличия ключа шифрования (см. пункт 6.8.2);
- условий проверки на основе шифрованной информации (см. пункт 6.8.3).

6.8.1 Степень шифрования

Любой "пакет" как протокольный блок данных состоит из управляющей информации протокола (PCI) и блока служебных данных (SDU) на разных уровнях протокола. При использовании шифрования на проверяемом тракте передачи сообщений оно может применяться:

- либо ко всему стеку протокола, либо только к его части (см. Примечание 1); и
- на одном из уровней протокола – либо к PDU уровня x (L_x) (т. е. ко всему L_x -PDU), либо только частично (например, лишь к L_x -PCI или L_x -SDU).

ПРИМЕЧАНИЕ 1. – Пример: услуга передачи пакетов RTP по протоколу IP может обеспечивать шифрование на:

- a) сетевом уровне (например, в транспортном режиме IPsec или туннельном режиме IPsec);
- b) транспортном уровне (например, с помощью DTLS); или/и
- c) прикладном уровне (например, с помощью SRTP).

DPI может осуществляться на любой нешифрованной части пакета.

R-6.8.1/1: Наличие информации о шифрованном трафике (с точки зрения сигнатуры DPI): DPI может факультативно осуществляться в отношении всех нешифрованных элементов информации проверяемого трафика, в зависимости от степени шифрования (см. Примечание 2).

ПРИМЕЧАНИЕ 2. – Пример: поток пакетов SRTP, передаваемых по протоколу IP, все еще может быть проверен в случае использования сигнатур DPI, основанных на элементах информации RTP PCI ("заголовок RTP"), UDP PCI ("заголовок UDP"), IP PCI ("пакет IP") и т. д., если зашифрован только RTP SDU (содержащий данные IP-приложения).

R-6.8.1/2: Отсутствие информации о шифрованном трафике (с точки зрения сигнатуры DPI): DPI может факультативно осуществляться как частичная DPI (потому что части сигнатур DPI могут быть соотнесены с нешифрованными элементами информации пакета).

Такая "частичная DPI" применительно к шифрованному трафику может означать "ограниченные услуги DPI", однако этого уже достаточно для конкретных случаев использования (например, если "грубой" идентификации приложения или протокола уже достаточно).

6.8.2 Наличие ключа дешифрования

R-6.8.2/1: DPI может факультативно применяться в случае локального наличия используемого(ых) ключа(ей) шифрования. В таком случае любая реализация DPI повлечет за собой предварительное дешифрование (локальной копии) проверяемого пакета.

6.8.3 Условия проверки на основе шифрованной информации

R-6.8.3/1: DPI может быть факультативно обеспечена в отношении шифрованного трафика в случае если политические условия применимы к проверкам на основе шифрованной информации (см. Примечание).

ПРИМЕЧАНИЕ. – Пример: любая комбинация битов (которая однозначно определяет какой-либо конкретный поток пакетов) может быть получена путем наблюдения (проверки) частично шифрованного трафика (см. пункт 6.8.1). В таком случае данная комбинация битов как часть последующих сигнатур DPI уже будет существовать в шифрованном коде.

6.8.4 Требования к DPI, относящиеся к IPsec

Требования, изложенные в подпунктах 6.8.1–6.8.4, действительны также для шифрованных пакетов IPsec. В настоящей Рекомендации внимание сосредоточено на аспектах идентификации потока шифрованного трафика IPsec. Аспекты, касающиеся идентификации приложения, подлежат дальнейшему изучению.

6.8.4.1 Общие требования

R-6.8.4.1/1: DPI-FE может факультативно обеспечивать возможность идентификации по меньшей мере *потока* шифрованного трафика IPsec. Соответствующий дескриптор потока, состоящий из *n* элементов, может быть факультативно ограничен элементами, относящимися только к уровням L2 и L3.

R-6.8.4.1/2: Поток может факультативно соответствовать трафику единственной ассоциации безопасности (SA) IPsec или может факультативно охватывать несколько SA.

R-6.8.4.1/3: Идентификация потока на основе SA означает, что 32-битовый индекс параметров безопасности (SPI) IPsec может факультативно являться частью дескриптора потока.

6.8.4.2 Транспортный и туннельный режимы IPsec

Протоколы IPsec (AH и ESP, см. ниже) могут использоваться для защиты либо всей полезной нагрузки IP (т. е. туннельный режим), либо протоколов верхнего уровня полезной нагрузки IP (т. е. транспортный режим).

R-6.8.4.2/1: DPI-FE может факультативно иметь возможность обнаружения шифрованного трафика IPsec в туннельном режиме.

R-6.8.4.2/2: DPI-FE может факультативно иметь возможность обнаружения шифрованного трафика IPsec в транспортном режиме.

6.8.4.3 Трафик IPsec, защищенный с помощью AH

Заголовок аутентификации (AH) обеспечивает целостность данных, аутентификацию источника данных и ограниченные факультативные услуги по предотвращению повторного использования пакетов (anti-replay).

R-6.8.4.3/1: DPI-FE может факультативно иметь возможность обнаружения трафика, защищенного с помощью AH, на основе соответствующего номера по протоколу IP.

6.8.4.4 Трафик IPsec, защищенный с помощью ESP

Инкапсуляция полезной нагрузки безопасности (ESP) обеспечивает дополнительную конфиденциальность.

R-6.8.4.4/1: DPI-FE может факультативно иметь возможность обнаружения трафика, защищенного с помощью ESP, на основе соответствующего номера по протоколу IP.

6.9 Проверка сжатого трафика

Сжатие предназначено для сокращения объема трафика. Например:

- сжатие методом "ZIP" [b-IETF RFC 1950] сокращает размер файлов (относится к потокам FTP по протоколу TCP/IP);
- сжатие методом "SigComp" [b-IETF RFC 3320] сокращает размер сообщений SIP (относится к потокам SIP по протоколу L4/IP).

6.9.1 Наличие информации о методе сжатия

R-6.9.1/1: DPI может факультативно обеспечиваться при наличии локальной информации о применяемой схеме сжатия (например, если узел DPI имеет информацию о том, что проверяемый тракт передачи сигнала SIP закодирован в соответствии с пунктом 8 [b-ETSI TS 124 229]). В таком случае любая реализация DPI повлечет за собой предварительное восстановление сжатой (локальной копии) проверяемого пакета.

R-6.9.1/2: DPI может также факультативно обеспечиваться при возможности извлечения информации о применяемой схеме сжатия из проверяемого потока трафика (например, информация о конкретном методе zip может быть факультативно извлечена из элементов информации заголовка файла).

6.10 Обнаружение необычного трафика

6.10.1 Требования к обнаружению необычного трафика

R-6.10.1/1: Требуется, чтобы DPI-FE мог обеспечивать обнаружение необычного трафика. А именно, требуется, чтобы сигнатуры DPI могли описывать обычный и необычный трафик (например, в виде черного или белого списка).

ПРИМЕЧАНИЕ. – Аспекты правила политики DPI: данная возможность может повлечь проверку многих метрик по характеристикам трафика и/или пакетов, а также возможное построение дерева решения для подготовки окончательного вывода относительно классов обычного и необычного трафика.

7 Функциональные требования с точки зрения сети

7.1 Общие требования

7.1.1 Электросвязь в чрезвычайных ситуациях

В целом, при разработке, реализации, развертывании и использовании функций DPI должны предусматриваться меры, направленные на предотвращение отрицательных последствий для показателей работы и безопасности применительно к электросвязи в чрезвычайных ситуациях (ЕТ). ЕТ [ITU-T Y.2205] означает любую услугу, связанную с чрезвычайными ситуациями, для которой требуется специальный режим, по сравнению с другими услугами (т. е. приоритетный режим по сравнению с обычными услугами). К ЕТ относятся службы экстренного вызова, уполномоченные властями, например, службы электросвязи в чрезвычайных ситуациях [ITU-T E.107] и службы общественной безопасности.

Настоящая Рекомендация основана на общем использовании маркера приложения для идентификации семантики различных приложений, такой как тип протокола приложения (например, видео МСЭ-Т H.264 или SIP, как пример протокола IP-приложения). Те же самые типы приложений (например, SIP) используются для поддержки как обычных услуг, так и прикладных услуг ЕТ. Вместе с тем в настоящей Рекомендации не определяется какой-либо уникальный маркер приложения для идентификации прикладных услуг ЕТ. В связи с этим потребуются надлежащие меры предосторожности, чтобы не допустить отрицательного воздействия на прикладные услуги ЕТ.

R-7.1/1: Требуется, чтобы не создавалось препятствий предоставлению приоритетного режима трафику прикладных услуг ЕТ по сравнению с обычными услугами.

R-7.1/2: Требуется, чтобы, в целом, при разработке, реализации, развертывании и использовании функций DPI предусматривались меры, направленные на предотвращение отрицательных последствий для показателей работы применительно к прикладным услугам ЕТ (например, создание ненужных задержек).

R-7.1/3: Требуется, чтобы, в целом, при разработке, реализации, развертывании и использовании функций DPI предусматривались меры по предотвращению нарушений безопасности, ставящих под угрозу целостность, конфиденциальность и доступность сообщений/сеансов ЕТ.

ПРИМЕЧАНИЕ. – В настоящей Рекомендации не содержится каких-либо положений относительно того, как должны соблюдаться указанные выше требования. Они могут выполняться путем использования функциональных возможностей, эксплуатационных мер или сочетанием обоих вариантов.

7.2 Плоскости данных, управления и контроля в узле DPI

7.2.1 Плоскости трафика и типы трафика с точки зрения узла DPI

В соответствии с сетевой моделью плоскости пользователя, контроля и управления (см. [b-ITU-T Y.2011]), узел DPI взаимодействует с трактом передачи данных и трактом принятия локального решения (см. рисунок 7-1). Трасс передачи данных может работать либо в однонаправленном режиме, либо в двунаправленном режиме.

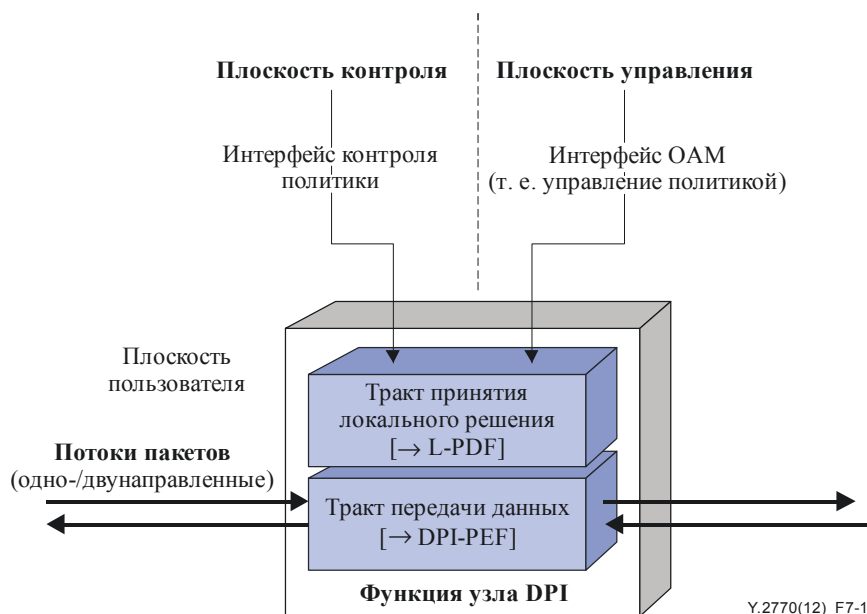


Рисунок 7-1 – Плоскости внешнего и внутреннего трафика узла DPI

ПРИМЕЧАНИЕ 1. – Потоки пакетов пересылаются с использованием маршрутизации/коммутации по тракту передачи пакетов, которые нередко называют трактами передачи данных в IP-сетях (см., например, [b-IETF RFC 4778]); в связи с этим термин "плоскость данных" является синонимом термин "плоскость пользователя".

ПРИМЕЧАНИЕ 2. – Трасс передачи IP-данных называют также IP медиатрактом (или трактом носителя) в случае трафика данных IP-приложения, или IP трактом передачи сигнала в случае трафика контроля приложения IP [b-ITU-T X.1141].

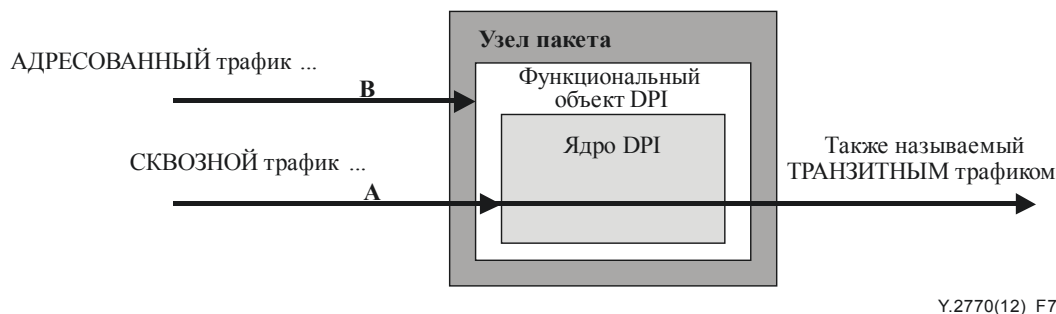
R-7.2.1/1: Требуется, чтобы узел DPI поддерживал интерфейс плоскости управления для управления политикой и мог факультативно поддерживать интерфейс плоскости контроля для контроля политики.

Объект тракта принятия локального решения обеспечивает внутренние возможности контроля и управления в узле.

R-7.2.1/2: Требуется, чтобы узел DPI распознавал два вида пакетов (см. рисунок 7-2):

- пакеты данных, которые принадлежат абонентам и в которых передается абонентский трафик (называемый "сквозным трафиком"; см. [b-IETF opsec]); и
- пакеты контроля и управления, которые принадлежат поставщику сети и имеют отношение к работе сети (называемый "адресованным трафиком"; см. [b-IETF opsec]).

Два типа пакетов передаются по "общему каналу" (или "в полосе") или передаются по разным каналам, в которых логически отделяются данные от "внеполосных" пакетов контроля (см. также [b-IETF RFC 4778], пункт 2.2 для примера трафика управления).



Y.2770(12)_F7-2

Рисунок 7-2 – Адресованный (А) и сквозной трафик (В) узла DPI

7.2.2 Требования, относящиеся к плоскости управления

R-7.2.2/1: Требуется, чтобы DPI-FE поддерживал протоколы управления для управления конфигурацией правил политики DPI.

R-7.2.2/2: Рекомендуется, чтобы DPI-FE поддерживал управление информацией об идентичности пользователя и взаимосвязь между пользователем и приложениями пользователя.

R-7.2.2/3: Рекомендуется, чтобы DPI-FE поддерживал управление приложениями и услугами:

- создание, изменение и публикацию шаблонов приложений;
- установление взаимосвязи между приложениями и стратегиями; и
- обеспечение резервирования услуги пользователя и управление ее резервированием;

R-7.2.2/4: Рекомендуется, чтобы DPI-FE поддерживал управление предварительно определенными или динамически создаваемыми стратегиями. (Эти стратегии могут факультативно относиться к идентификации приложения, контролю приложения и управлению пользователями).

R-7.1.2/5: Рекомендуется, чтобы DPI-FE поддерживал управление административными полномочиями. В целях обеспечения иерархического управления у разных администраторов имеются разные управленческие полномочия.

7.2.3 Требования, относящиеся к плоскости контроля

R-7.2.3/1: DPI-FE может факультативно поддерживать протоколы управления политикой (например, [b-ITU-T H.248.1] для эталонной точки МСЭ-Т R_w, определенной в [ITU-T Y.2111]), в целях контроля и передачи сигналов правил политики DPI.

7.2.4 Требования, относящиеся к плоскости (данных) пользователя

Плоскость данных (пользователя) отвечает следующим факультативным требованиям:

R-7.2.4/1: DPI-FE может факультативно поддерживать различные пакетные технологии (например, xDSL, UMTS, CDMA2000, кабельные технологии, LAN, WLAN, Ethernet, MPLS, IP, ATM).

7.2.5 Требования ко всем плоскостям

R-7.2.5/1: DPI-FE может факультативно поддерживать согласованную грамматику протокола для определения правил политики DPI. Рекомендуется, чтобы синтаксис, используемый в интерфейсе контроля политики (плоскость контроля) и в интерфейсе управления политикой (плоскость управления), был преимущественно идентичным. Данная рекомендация не подразумевает использования одного и того же протокола, однако касается языка описания правил политики (DPI) (который нередко называется языком описания фильтров (FSL) или языком описания политики (PSL); см. Примечание).

ПРИМЕЧАНИЕ. – Примерами языков описания сценариев являются языки SIEVE [b-IETF RFC 5228], PERL, XML и XACML (расширяемый язык разметки, предусматривающий контроль доступа).

Согласованная грамматика протокола позволяет использовать общую модель данных/объектов в тракте реализации политики в рамках узла DPI, что является обязательным условием эффективного и быстрого исполнения правил, а также бесперебойных операций по обновлению библиотеки сигнатур DPI.

8 Интерфейсы функционального объекта DPI

Требования, описанные в предыдущих пунктах, приводят к следующим интерфейсам:

- между DPI-FE и удаленным объектом сети (см. пункт 8.1); и
- между внутренними компонентами DPI-FE (см. пункт 8.2).

8.1 Внешние интерфейсы DPI-FE

На рисунке 8-1 изображены внешние интерфейсы DPI-FE:

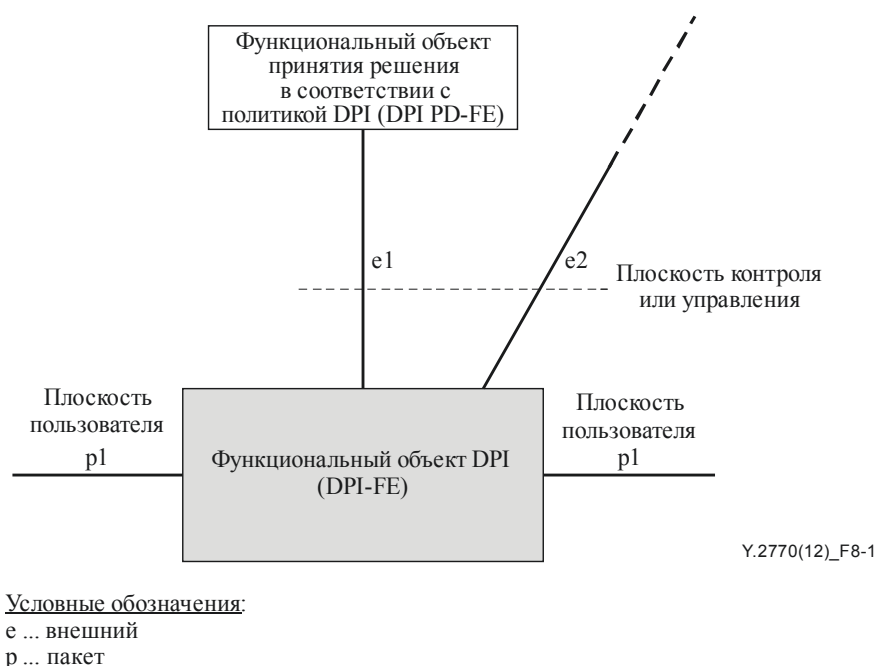


Рисунок 8-1 – Внешние интерфейсы DPI-FE

8.1.1 Проверяемый трафик (p1)

DPI-FE обменивается пакетами с удаленными узлами пакетов через интерфейс *p1*. Топология тракта передачи пакетов является топологией типа "пункт-пункт" для DPI-FE, действующего в режиме *DPI на тракте*. Топологии типа "много пунктов – много пунктов" не поддерживаются. Интерфейс *p1* охватывает *двунаправленные* тракты передачи пакетов.

Топология тракта передачи пакетов для DPI-FE, действующего в режиме *DPI вне тракта*, относится к конечному пункту.

8.1.2 Контроль проверки трафика/управление проверкой трафика (e1)

Функциональный объект принятия решения в соответствии с политикой DPI (DPI-PDFE) предназначен для контроля или управления DPI-FE. Таким образом, информация, обмен которой осуществляется через *e1*, касается команд, предназначенных для контроля/конфигурации режима обработки пакетов DPI-FE. Такие команды могут быть описаны в политике DPI.

Интерфейс *e1* может также поддерживать представление отчетов и уведомлений от DPI-FE в направлении к DPI-PDFE.

8.1.3 Предоставление отчетности другим сетевым объектам (e2)

Интерфейс *e2* охватывает все возможные интерфейсы связи с удаленными сетевыми объектами, за исключением DPI-PDFE. Этот интерфейс поддерживает, в основном, предоставление отчетности.

8.2 Внутренние интерфейсы DPI-FE

На рисунке 8-2 представлены возможные внутренние интерфейсы, основанные на требованиях DPI:

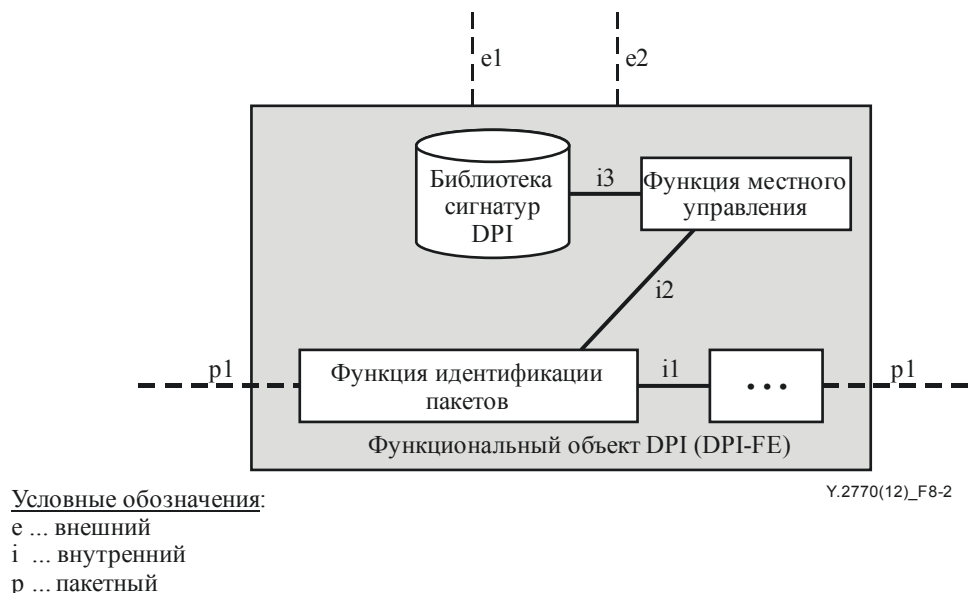


Рисунок 8-2 – Внутренние интерфейсы DPI-FE

Могут присутствовать также и другие внутренние функциональные компоненты и внутренние интерфейсы DPI-FE. Внутренние интерфейсы являются предметом для дополнительного изучения.

8.3 Требования к интерфейсам

R-8.3/1: Рекомендуется, чтобы интерфейс *e1* придерживался требований, упомянутых в пункте 6.5.

R-8.3/2: Рекомендуется, чтобы интерфейс *e2* придерживался требований, упомянутых в пункте 6.4.1.

9 Соображения и требования безопасности

В данном пункте содержится описание угроз безопасности и определяются требования безопасности для объектов DPI в СПП.

9.1 Угрозы безопасности объектам DPI

Функциональные объекты, связанные с DPI, могут обычно находиться в *доверенной зоне* или *доверенной, но уязвимой зоне* оператора СПП, как это определено в [ITU-T Y.2701]. В настоящей Рекомендации определяются угрозы безопасности СПП, а также требования, касающиеся защиты от этих угроз. Поскольку объекты, связанные с DPI, являются частью СПП, то к ним применимы выводы [ITU-T Y.2701]. Исходя из [ITU-T Y.2701], требования безопасности, относящиеся к объектам DPI, определяются следующим образом:

- уничтожение информации, относящейся к DPI;
- искажение или изменение информации, относящейся к DPI;
- хищение, удаление или потеря информации, относящейся к DPI;
- раскрытие информации, относящейся к DPI;
- прерывание обслуживания.

Информация, относящаяся к операциям по DPI, включает правила политики для DPI с их сигнатурами, информацию об экспортированном потоке DPI и информацию о приложении.

Уничтожение, искажение или изменение, хищение, удаление и потеря такой информации могут сделать ее непригодной для операций DPI. Во многих странах такую информацию рекомендуется обрабатывать в соответствии с национальными регламентарными требованиями и требованиями политики, при этом она не должна раскрываться.

Прерывание обслуживания может стать результатом атак "отказ в обслуживании" DoS. Любой объект, принимающий данные, может стать мишенью атаки DoS. Например, злоумышленник может опосредованным образом наводнить объект DPI большим объемом трафика, ухудшая, тем самым, качество обслуживания или прерывая услуги DPI для законных пользователей.

9.2 Требования безопасности для объектов DPI

Основными требованиями безопасности для объектов DPI являются:

R-9.2/1: Информация, относящаяся к DPI и находящаяся в объектах DPI, должна быть защищена.

R-9.2/2: Если обмен информацией осуществляется за пределами *доверенной зоны* оператора СПП, то информация, относящаяся к DPI, должна быть защищена между объектами DPI и удаленными функциональными объектами (например, DPI PD-FE, NMS)

R-9.2/3: В некоторых случаях могут потребоваться механизмы для ослабления лавинных атак против DPI FE.

R-9.2/4: При выполнении настоящей Рекомендации поставщики оборудования, операторы сетей и поставщики услуг должны учитывать национальные регламентарные требования и требования политики.

R-9.2/5: Конструкторам рекомендуется использовать существующие тщательно проверенные механизмы для удовлетворения требований безопасности, предусмотренных в настоящей Рекомендации. Например, как это определено в Рекомендации МСЭ-Т Y.2704 [ITU-T Y.2704].

Приложение А

Описание дескриптора потока

(Данное приложение является неотъемлемой частью настоящей Рекомендации.)

А.1 Синтаксическая перспектива протокола

Дескриптор потока имеет отношение к структуре данных (объекту данных), которая может быть смоделирована как набор из k элементов (см. рисунок А.1). Структура данных состоит из информационных элементов k (IE) (Примечание). Значение k колеблется и составляет больше нуля¹, однако для данного конкретного потока оно является постоянным. Элементы информации – это элементы, содержащиеся в реестре IANA IPFIX. Существует значение, связанное с каждым элементом информации. Ассоциация – это типично математическое равенство ('='), однако не исключаются и другие математические зависимости.

ПРИМЕЧАНИЕ. – Элементу информации IETF IPFIX может быть присвоен атрибут "ключевого поля" или "неключевого поля".

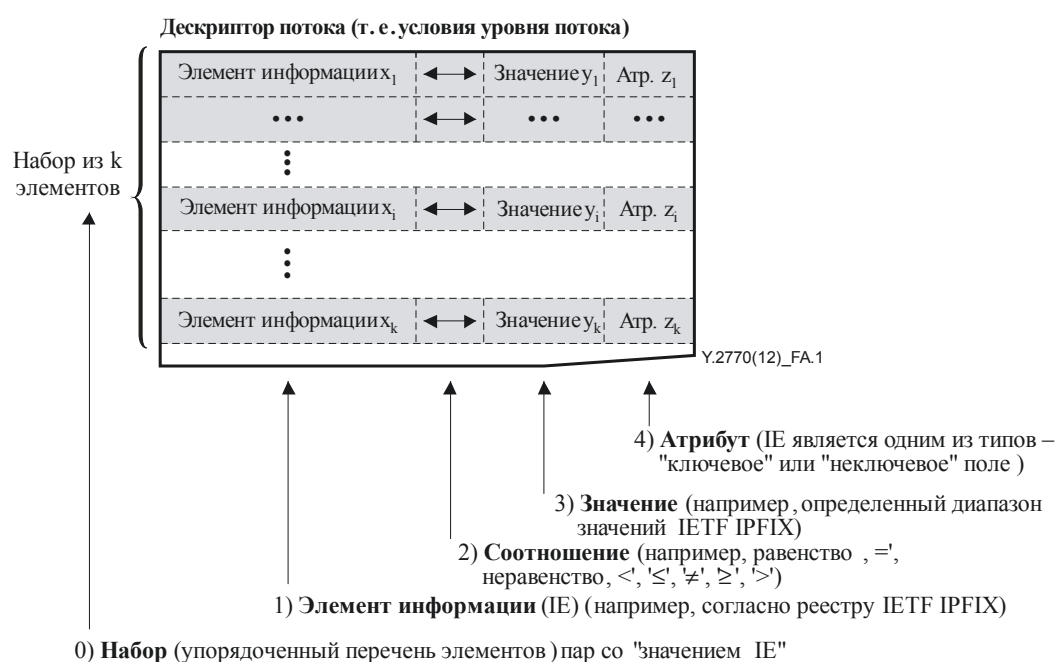


Рисунок А.1 – Дескриптор потока (условия уровня потока) с синтаксической точки зрения протокола

Таким образом, дескриптор уровня потока, как набор из k чисел, представляет собой перечень k "пар имя-значение" (NVP); здесь последовательность "< IE ↔ значение >" пары².

А.2 Определение значений элементов информации

В условиях уровня потока значение IE может быть:

- Полностью определено

Полная спецификация представляет собой случай полной настройки имя-значение.

¹ Примечание: $N = 0$ указывает – "независящий от потока".

² Аналогично другим структурам, таким как AVP (<наименование, значение атрибута>), пара параметр-значение (<параметр=значение>) и т. д.

- Не определено.
"Не определено" представляет собой случай, когда *еще нет* какого-либо значения, присвоенного IE.
- Переопределено.
Переопределение указывает на то, что существует множество возможных значений для данного конкретного IE.
- Недоопределено.
Недоопределение указывает на обобщение (например, все возможные значения или выбор значения).

А.3 Связь между дескриптором потока, идентификатором потока IPFIX и ключом потока IPFIX

Пример на рисунке А.2 представляет дескриптор потока из 5 элементов и содержит 5 ключей потока IPFIX. Чтобы определить конкретный поток, дескриптор потока устанавливает некоторые условия для значений этих ключей потока, как это определено в пункте А.2: первый ключ потока IE x_1 "полностью определен", второй ключ потока IE x_2 "переопределен", в то время как другие IE "не определены", как показано в части а) рисунка А.2.

а) ... Условия уровня потока, которые могут частично представлять информацию ключей IPFIX, предоставлены для DPI-FE ...

Дескриптор потока

IE x_1	=	Полностью определен y_1	"Ключ"
IE x_2	>	Переопределен y_2	"Ключ"
IE x_3		Не определен	"Ключ"
IE x_4		Не определен	"Ключ"
IE x_5		Не определен	"Ключ"

5 ключей потока IPFIX

б) ... Обработка DPI ведет к идентификации всех наблюдаемых значений для IE ...

Идентификатор потока IPFIX (Примечание)

IE x_1	Наблюдаемое значение y_1	"Ключ"
IE x_2	Наблюдаемое значение y_2	"Ключ"
IE x_3	Наблюдаемое значение y_3	"Ключ"
IE x_4	Наблюдаемое значение y_4	"Ключ"
IE x_5	Наблюдаемое значение y_5	"Ключ"

в) ... DPI-FE в итоге может сообщить информацию об идентифицированном потоке (например, идентификатор потока IPFIX)

Y.2770(12)_FA.2

ПРИМЕЧАНИЕ. – Идентификатор потока IPFIX является объектом, полученным из дескриптора потока, и поэтому он не повлияет на контент дескриптора потока.

Рисунок А.2 – Пример дескриптора потока, идентификатора потока IPFIX и ключей потока IPFIX

Следует отметить, что дескриптор потока не устанавливает условия только для ключей потока IPFIX: в самом деле, при некоторых обстоятельствах могут потребоваться дескрипторы потока на ключе, не связанном с потоком, например, когда требуется состояние флагов TCP первого пакета потока. Принципиальное отличие между дескриптором потока и идентификатором потока IPFIX в примере на рисунке А.2 состоит в том, что дескриптор потока содержит "больше, чем" условие на $IE\ x_2$, (" $IE\ x_2 > \text{значение } y_2$ ") , в то время как идентификатор потока IPFIX содержит наблюдаемое значение для $IE\ x_2$, т. е. значение y_2 . Идентификатор потока IPFIX состоит из набора наблюдаемых значений для ключей потока, после того как функциональный объект DPI обработал пакеты и распределил их в потоке.

Следует отметить, что, если экспортированная информация (например, через запись о потоке IPFIX) содержит IE вместе с соответствующими наблюдаемыми значениями и, независимо от того, является ли соответствующий IE ключом потока IPFIX или нет, то нет никакой необходимости присваивать конкретный идентификатор потока IPFIX, поскольку идентификатор потока IPFIX является общим итогом всей этой информации.

Библиография

- [b-ITU-T H.248.1] Рекомендация МСЭ-Т H.248.1, версия 3 (2005 г.), *Протокол управления шлюзом: Версия 3.*
- [b-ITU-T X.734] Рекомендация МСЭ-Т X.734 (1992 г.), *Информационные технологии – Взаимосвязь открытых систем – Управлением системами: Функции управления сообщениями и событиями.*
- [b-ITU-T X.1141] Рекомендация МСЭ-Т X.1141 (2006 г.), *Язык разметки, предусматривающий защиту данных (SAML 2.0).*
- [b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*
- [b-ITU-T Y.2121] Recommendation ITU-T Y.2121 (2008), *Requirements for the support of flow-state-aware transport technology in NGN.*
- [b-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture.*
- [b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10).*
- [b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9).*
- [b-IETF IANA IPFIX] IETF IANA IPFIX (2007), *IP Flow Information Export (IPFIX) Entities.*
<<http://www.iana.org/assignments/ipfix/ipfix.xhtml>>
- [b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure.*
<<http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>>
- [b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3.*
- [b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management.*
- [b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp).*
- [b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*
- [b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol.*
- [b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.*
- [b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB.*
- [b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments.*
- [b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.*
- [b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export.*
- [b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX).*
- [b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language.*

- [b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.
- [b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.
- [b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.
- [b-PacketTypes] McCann, P.J., and Chandra S. (2000), *Packet Types: Abstract Specification of Network Protocol Messages*; in SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
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 и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи