Международный союз электросвязи

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2771
(07/2014)

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

Сети последующих поколений – Безопасность

# Структура углубленной проверки пакетов

Рекомендация МСЭ-Т Y.2771

ITU-T

Международный союз электросвязи

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.*

# Рекомендация МСЭ-T Y.2771

## Структура углубленной проверки пакетов


**Резюме**

В Рекомендации МСЭ-T Y.2771 представлена структура углубленной проверки пакетов (DPI). Основным назначением этой структуры является описание структурированного подхода к разработке, определению и реализации решений по DPI для обеспечения информированности об услуге/приложении в целях содействия функциональной совместимости в развивающихся сетях. Она способствует определению и облегчению понимания связанных с сетями вопросов, в первую очередь в свете архитектуры. В настоящей Рекомендации также представлены аспекты структуры DPI с позиций моделирования и качества.

Подобные структуры предназначены главным образом для описания возможных взаимосвязей между функцией DPI и другими функциями сети, с тем чтобы содействовать определению требований к функциям DPI (которые сами по себе являются объектом рассмотрения для других Рекомендаций МСЭ-T, например [ITU-T Y.2770]) и способствовать работе с терминологией (например, при сопоставлении того или иного определения с функциональной моделью).



**Хронологическая справка**

| Издание | Рекомендация | Утверждение | Исследовательская комиссия | Уникальный идентификатор* |
|---|---|---|---|---|
| 1.0 | МСЭ-T Y.2771 | 18.07.2014 г. | 13-я | 11.1002/1000/12178 |


* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: 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 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/.

## СОДЕРЖАНИЕ

# Рекомендация МСЭ-Т Y.2771

## Структура углубленной проверки пакетов

### 1 Сфера применения

В настоящей Рекомендации представлена структура углубленной проверки пакетов (DPI) в пакетных сетях. Важнейшим назначением данной Рекомендации является описание основных концепций, функциональных компонентов и возможностей DPI, которые могут использоваться для идентификации информационных потоков в пакетных сетях при помощи объектов DPI в целях поддержки спецификации требований DPI и определения структурированных решений для пакетных сетей (таких как СПП).

В настоящей Рекомендации представлена системная информация высокого уровня относительно основных принципов, которые, как правило, соблюдаются при реализации объектов DPI. Однако в документ не планируется включать полный комплект подробных спецификаций для DPI. Скорее настоящая Рекомендация представляет информацию высокого уровня (т. е. структуру) и предназначена для использования в качестве справочного материала в работе Исследовательских комиссий МСЭ и других групп экспертов, не входящих в МСЭ, например в качестве исходных данных для разработки или детализированных стандартов функциональных возможностей DPI.

Сфера применения настоящей Рекомендации включает:

a) основные архитектурные принципы, которые будут встречаться при комбинировании DPI в различных сетевых архитектурах;

b) архитектурные аспекты протоколов с точки зрения DPI;

c) типовые функциональные модели и их применение в сценариях использования DPI; и

d) структуры показателей работы в целях оказания помощи при обсуждении показателей DPI, таких как идентификация ключевых эксплуатационных показателей, относящихся к DPI.

Пользователи и специалисты по применению этой Рекомендации МСЭ-Т должны соблюдать все действующие государственные и региональные законы, нормативные акты и политические принципы. Механизм, описанный в настоящей Рекомендации, может не применяться в отношении международной корреспонденции, с тем чтобы обеспечить конфиденциальность и выполнение суверенных национальных юридических требований, которые возложены на поставщиков электросвязи, а также соблюдения Устава и Конвенции МСЭ.

### 2 Справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и других справочных документах содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования действовали указанные редакции документов. Все Рекомендации и другие справочные документы являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочных документов, перечисленных ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т.

Ссылка на документ в рамках этой Рекомендации не дает ему как отдельному документу статуса рекомендации.

[ITU-T E.800] Рекомендация МСЭ-Т E.800 (2008), *Определение терминов, относящихся к качеству обслуживания*.

[ITU-T G.602] Recommendation ITU-T G.602 (1988), *Reliability and availability of analogue cable transmission systems and associated equipments*.

[ITU-T H.248.86] Рекомендация МСЭ-Т H.248.86 (2014), *Протокол управления шлюзом: H.248 Поддержка углубленной проверки пакетов*.

[ITU-T X.200] Рекомендация МСЭ-Т X.200 (1994), *Информационные технологии – Взаимосвязь открытых систем – Базовая эталонная модель: Базовая модель*.

[ITU-T X.731] Рекомендация МСЭ-Т X.731 (1992), *Информационные технологии – Взаимосвязь открытых систем – Управлением системами: Функция управления состоянием*.

[ITU-T Y.2704] Рекомендация МСЭ-Т Y.2704 (2007), *Механизмы и процедуры безопасности для сетей последующих поколений*.

[ITU-T Y.2770] Рекомендация МСЭ-Т Y.2770 (2012), *Требования к углубленной проверке пакетов в сетях последующих поколений*.

[ETSI TS 132.410] ETSI TS 132 410 (10/2012), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM (3GPP TS 32.410 version 11.0.0 Release 11)*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6)*.

[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 приложение (application)** [ITU-T Y.2770]. Обозначает одно из следующих понятий:

- тип протокола приложения (например, протоколы IP-приложений, видео МСЭ-Т H.264 или протокол инициирования сеанса связи (SIP));
- отдельный случай обслуживаемого пользователя (например, VoIP, VoLTE, VoIMS, VoNGN и VoP2P), относящийся 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); и
- 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 стандартного выражения в качестве "условий прикладного уровня", см. также п. 3.2.2 [ITU-T Y.2770]), в виде общих характеристик всех перечисленных выше уровней приложений.

**3.1.2 готовность (availability)** [ITU-T E.800]. Готовность элемента быть в состоянии выполнить требуемую функцию в данный момент времени или в любой момент времени в рамках заданного временного интервала в предположении предоставления, если необходимо, внешних ресурсов.

**3.1.3 дескриптор приложения (application descriptor) (также называемый условиями прикладного уровня (application-level conditions))** [ITU-T Y.2770]. Набор условий правил, который идентифицирует приложение (в соответствии с п. 3.2.1 [ITU-T Y.2770]).

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.

**3.1.4 углубленная проверка пакетов (deep packet inspection (DPI))** [ITU-T Y.2770]. 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. п. 3.2.11 [ITU-T Y.2770] 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 предоставление отчета, или в действиях в отношении пакета.

**3.1.5 ядро DPI (DPI engine)** [ITU-T Y.2770]. 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 [ITU-T Y.2770]).

**3.1.6 условие политики DPI (DPI policy condition) (также называемое сигнатурой DPI (DPI signature))** [ITU-T Y.2770]. Представление необходимого состояния и/или предварительных условий, по которым идентифицируется приложение и определяется необходимость выполнения действий, предусмотренных 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.

**3.1.7 функциональный объект принятия решения в соответствии с политикой DPI (DPI policy decision functional entity)** (DPI-PDFE) [ITU-T Y.2770]. 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.

**3.1.8 дескриптор потока (flow descriptor) (также называемый условиями уровня (level conditions))** [ITU-T Y.2770]. Набор условий правила, которые используются для идентификации конкретного типа потока (в соответствии с п.3.1.3 [ITU-T Y.2770]) в проверяемом трафике.

ПРИМЕЧАНИЕ 1. – Настоящее определение дескриптора потока расширяет определение, приведенное в [b-ITU-T Y.2121], за счет дополнительных элементов, описанных в п. 3 [ITU-T Y.2770].

ПРИМЕЧАНИЕ 2. – Дополнительное обсуждение нормативных аспектов дескриптора потока, используемого в [ITU-T Y.2770], приведено в Приложении A к [ITU-T Y.2770].

**3.1.9 Надежность (reliability)** [ITU-T E.800]. Вероятность того, что элемент может выполнять требуемую функцию при определенных условиях в течение заданного периода времени.

### 3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

**3.2.1 Анализатор DPI (DPI analyser)**. Последующий объект в тракте обработки DPI (в рамках функции реализации политики DPI), ориентированный на функции сравнения между заголовками определенных пакетов и полезными нагрузками предварительно отобранных потоков пакетов. Основная сфера применения анализатора DPI связана с оценкой *условий* политики DPI по сравнению с *предварительно отобранными* входящими пакетами.

ПРИМЕЧАНИЕ. – Анализатор DPI может располагаться после сканера DPI (см. п. 3.2.6). Анализатор DPI может обеспечивать функции анализатора системы обнаружения проникновения (IDS).

**3.2.2 Узел DPI**. Сетевой элемент или устройство, реализующее функции, связанные с DPI. Таким образом, это общий термин, который используется для обозначения реализации физического объекта DPI.

ПРИМЕЧАНИЕ. – С функциональной точки зрения функция узла DPI (DPI-NF) включает функцию реализации политики DPI (DPI-PEF) и (факультативно) локальную функцию принятия решений в соответствии с политикой (L-PDF), следовательно, DPI-NF функционально эквивалентна функциональному объекту DPI.

**3.2.3 Действие в соответствии с политикой DPI (DPI policy action) (сокращенно – действие).** Определение необходимого действия для реализации правила политики при соблюдении условий этого правила. Действия в соответствии с политикой могут привести к тому, что выполнение одной или нескольких операций может повлиять на сетевой трафик и сетевые ресурсы и/или изменить их конфигурацию, см. также в [b-IETF RFC 3198].

**3.2.4 Функция реализации политики DPI (DPI policy enforcement function) (DPI-PEF).** Логический объект, обеспечивающий принятие связанных с политикой решений, заданных правилами политики DPI.

**3.2.5 Сканер DPI (DPI scanner) (используется также в качестве "функции сканирования DPI").** Первый объект в тракте обработки DPI (в рамках функции реализации политики DPI), обеспечивающий предварительный отбор (по отношению к последующему анализатору DPI, см. п. 3.2.8) путем выбора *всех условий* политики DPI в отношении *всех* входящих пакетов.

**3.2.6 Группа избыточности DPI "1+N".** Группа функциональных компонентов DPI (например, узел DPI, DPI-PIB, ядро DPI и т. д.), соответствующая архитектуре избыточности "1+N" (и $N \geq 1$), заданная одиночным рабочим компонентом и N защитными компонентами.

ПРИМЕЧАНИЕ. – Указанная выше группа используется для обеспечения дополнительной надежности и повышения готовности для узла DPI или сети, развернутой с одним из узлов DPI.

# 4 Сокращения и акронимы

## 4.1 Основные сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

| | | |
|---|---|---|
| $A_{DPI}$ | DPI policy action | Действие в соответствии с политикой DPI |
| BRM | Basic Reference Model | Базовая эталонная модель |
| CAM | Content Addressable Memory | Ассоциативное запоминающее устройство |
| $C_{DPI}$ | DPI policy condition | Условие политики DPI |
| DAI | Deep Application Identification | Углубленная идентификация приложений |
| DHI | Deep Header Inspection | Углубленная проверка заголовков |
| DiffServ | Differencial Service | Дифференцированная услуга |
| DPI | Deep Packet Inspection | Углубленная проверка пакетов |
| DPI-AcEF | DPI Action Execution Function | Функция выполнения действия DPI |
| DPI-AnF | DPI Analyser Function | Функция анализатора DPI |
| DPI-FE | DPI Functional Entity | Функциональный объект DPI |
| $DPI_{InP}$ | In-Path DPI | DPI в тракте |
| DPI-NF | DPI Node Function | Функция узла DPI |
| $DPI_{OoP}$ | Out-of-Path DPI | DPI вне тракта |

| | | |
|---|---|---|
| DPI-PDFE | DPI Policy Decision Function Entity | Функциональный объект принятия решений в соответствии с политикой DPI |
| DPI-PE | DPI Physical Entity | Физический объект DPI |
| DPI-PEF | DPI Policy Enforcement Function | Функция реализации политики DPI |
| DPI-PIB | DPI Policy Information Base | База информации о политике DPI |
| DPI-PIF | DPI Packet Identification Function | Функция идентификации пакетов DPI |
| DPI-ScF | DPI Scan Function | Функция сканирования DPI |
| DNNF | Determining Next Node Function | Функция определения следующего узла |
| FIB | Forwarding Information Base | База информации о пересылке |
| FTP | File Transfer Protocol | Протокол передачи файлов |
| HTTP | Hyper-Text Transport Protocol | Протокол передачи гипертекста |
| HW | HardWare | Аппаратное обеспечение |
| IDS | Intrusion Detection System | Система обнаружения проникновения |
| IP | Internet Protocol | Интернет-протокол |
| IPFIX | IP Flow Information Export | Экспорт информации о потоках IP |
| KPI | Key Performance Indicator | Ключевой показатель работы |
| $KPI_{DPI}$ | Key performance indicators for DPI entities | Ключевые показатели работы для объектов DPI |
| L-PDF | Local PDF | Локальная PDF |
| L2VPN | Layer 2 Virtual Private Network | Виртуальная частная сеть второго уровня |
| $L_XHI$ | Header Inspection of protocol Layer X | Проверка заголовка протокола уровня X |
| $L_XPI$ | Payload Inspection of protocol Layer X | Проверка полезной нагрузки протокола уровня X |
| LX | (Protocol) Layer X | Уровень X (протокола) |
| LX+ | Higher (Protocol) Layer than LX | Более высокий уровень (протокола), чем LX |
| MIB | Management Information Base | Информационная база управления |
| MPI | Medium depth Packet Inspection | Средняя проверка пакетов |
| MPLS | Multi-Protocol Label Switch | Многопротокольная коммутация с использованием меток |
| MTBF | Mean Time Between Failure | Среднее время наработки на отказ |
| MTTR | Mean Time To Repair | Среднее время ремонта |
| NA(P)T | Network Address (and Port) Translation | Преобразование сетевых адресов и портов |
| NGN | Next Generation Network | Сеть последующих поколений (СПП) |
| OSI-BRM | Open System Interconnection-Basic Reference Model | Взаимосвязь открытых систем – базовая эталонная модель |
| PDF | Policy Decision Function | Функция принятия решений в соответствии с политикой |
| PEP | Policy Enforcement Point | Точка реализации политики |
| PFF | Packet Forwarding Function | Функция пересылки пакетов |
| PIB | Policy Information Base | База информации о политике |
| QoS | Quality of Service | Качество обслуживания |
| RACF | Resource and Admission Control Functions | Функции управления ресурсами и допуском |
| $R_{DPI}$ | DPI policy rule | Правило политики DPI |
| R-PDF | Remote PDF (i.e., PDF remotely located from DPI node perspective) | Удаленная функция PDF (т. е. PDF, расположенная на расстоянии с точки зрения узла DPI) |

| | | |
|---|---|---|
| RTSP | Real Time Streaming Protocol | Протокол потоковой передачи в реальном времени |
| SDU | Service Data Unit | Блок служебных данных |
| SIP | Session Initiation Protocol | Протокол инициирования сеанса |
| SPI | Shallow Packet Inspection | Поверхностная проверка пакетов |
| $S_D$-PDF | Session-dependent PDF | PDF, зависящая от сеанса |
| $S_I$-PDF | Session-independent PDF | PDF, не зависящая от сеанса |
| SW | Software | Программное обеспечение |
| TCAM | Ternary Content Addressable Memory | Троичное ассоциативное запоминающее устройство |
| TCP | Transmission Control Protocol | Протокол управления передачей |
| TOS | Type of Service | Тип услуги |
| VoIP | Voice over IP | Передача голоса по IP |
| VoLTE | Voice over Long Term Evolution | Передача голоса по технологии долгосрочной эволюции (LTE) |
| VoIMS | Voice over Integrated Media System | Передача голоса через интегрированную медиасистему |
| VoNGN | Voice over Next Generation Network | Передача голоса по сетям последующих поколений |
| VoP2P | Voice over Peer to Peer | Передача голоса по одноранговым сетям |

## 4.2 Математические символы

В настоящей Рекомендации используются следующие символы (название, единица измерения и краткое описание).φ

| | | |
|---|---|---|
| $\varepsilon_{DPI}$ | (DPI) Коэффициент ошибок | – |
| $\varepsilon_{f-n}$ | (DPI) Коэффициент ложноотрицательных ошибок | – |
| $\varepsilon_{f-p}$ | (DPI) Коэффициент ложноположительных ошибок | – |
| $\varphi_{P,\,In}$ | (DPI) Скорость обработки входящих пакетов | [$s^{-1}$] |
| $\varphi_{P,\,Out}$ | (DPI) Скорость пакетов в исходящем направлении | [$s^{-1}$] |
| $\varphi_{P,\,Node,\,Out}$ | Пропускная способность узла передачи пакетов | – |
| $\varphi_{P,\,Identified}$ | Коэффициент успешно идентифицированных пакетов | – |
| $P_{Hit,\,BloomFilter}$ | Достоверность вероятности расчетных данных | – |
| $N_{db}$ | Количество правил политики DPI | – |
| $S_p$ | Размер пакета | – |
| $N_{DPIeng}$ | Количество ядер DPI | – |
| $\tau_{TD}$ | Задержка передачи внутри узла (узла DPI) | [ns] |
| $\underline{A}$ | Набор действий в соответствии с правилами (политики DPI) | – |
| $\underline{\underline{C}}$ | Набор условий правил (политики DPI) | – |
| $\underline{\underline{R}}$ | Набор правил (политики DPI) | – |

# 5 Условные обозначения

Отсутствуют.

## 6 Архитектурная концепция

### 6.1 Архитектурная концепция сети – сетевые сценарии высокого уровня

В данной концепции кратко изложены основные граничные условия развертывания DPI в сетевой инфраструктуре. Некоторые принципиальные сценарии концепции DPI могут быть идентифицированы путем рассмотрения таких критериев, как:

- **уровень расположения в сети** (т. е. расположение объекта DPI в домене пакетной сети):
  - на границе (**граничный уровень DPI**), или
  - в пределах сети (**базовый уровень DPI**),
  - между одноранговыми сетями (**одноранговый уровень DPI**);
- **типы сетевых пакетов (с точки зрения трактов)** (т. е. категория проверяемых типов пакетов[1]):
  - плоскость пользователя (или страта транспортирования; например, IP-тракт передачи данных, IP-медиатракт, IP-тракт носителя, туннель, MPLS LSP, псевдопровод и т. д.), или
  - плоскость контроля (или страта обслуживания; например, IP-тракт сигнализации), или
  - плоскость управления, или
  - комбинированные варианты;
- **приведение уровня в соответствие с другими сетевыми архитектурами** (имеется в виду уровень, на котором объект DPI сочетается с базовой архитектурой пакетной сети):
  - **изолированный** объект **DPI** (т. е. объект DPI, скрытый для пакетной сети).

    Примеры:
    - небольшое количество объектов DPI, расположенных в выбранных точках сети (перед которыми не стоит задача обеспечить "полное покрытие"; нечто вроде "DPI в тракте" в режиме зондирования),
    - объекты DPI вне тракта;
  - **наложенная сеть DPI** (т. е. существует специальная инфраструктура сети DPI, наложенная на базовую пакетную сеть; обе сетевые инфраструктуры с функциональной точки зрения являются раздельными).

    Примеры:
    - общий пример – сеть объектов DPI в тракте, использующих, например, тракты плоскости пользователя совместно, а интерфейсы контроля и/или управления – раздельно;
    - конкретный пример – например, функция DPI в целях обнаружения проникновения;
  - **встроенный объект DPI** (т. е. функциональный объект DPI встраивается в физический сетевой элемент совместно с другими функциональными объектами, относящимися к обработке пакетов, не связанной с DPI; подобный физический объект должен предоставлять, например, единственный интерфейс OAM с точки зрения экономически эффективной эксплуатации, что в свою очередь подразумевает согласованную модель управления на всех функциональных объектах).

    Примеры:
    - общий пример – объект DPI с информационной базой управления, которая приведена в соответствии с базой управления других функциональных объектов того же физического сетевого элемента, не связанных с DPI;
    - конкретный пример – функциональный объект DPI в рамках RACF и общие возможности управления, но без совместного использования каких-либо управляющих интерфейсов RACF;

---

[1] Понятие "тип пакета" может быть конкретизировано в соответствии с выделенным "протоколом" или "стеком протоколов". Однако подобный уровень детализации в данном случае не требуется.

− **интегральная DPI** (т. е. объект DPI, "полностью интегрированный" в "пакетную сеть").

Примеры:

- общий пример – эталонная модель (архитектура) сети, определяемой SDO, которая учитывает объекты DPI;
- конкретный пример – функция RACF МСЭ-Т, расширенная за счет объектов DPI (которые могут использовать существующие эталонные точки (например, "DPI, управляемая Rw" или Rw на базе МСЭ-Т H.248 с расширением при поддержке [ITU-T H.248.86]), или могут применять новые эталонные точки).

Таким образом, существует множество вариантов использования объекта DPI с точки зрения сценария сетевой интеграции.

## 6.2 Архитектурная концепция протокола – уровень проверки пакетов для некоторых типовых сетевых приложений

### 6.2.1 Принцип

Существуют различные уровни проверки пакетов. В таблице 6-1 приведен обзор типичных сетевых приложений в отношении необходимого применения "уровней проверки пакетов". Уровень проверки пакетов может быть обозначен или

1 согласно базовой эталонной модели (BRM) для многоуровневых архитектур протоколов, здесь − столбцы $L_x$HI и $L_y$PI; или

2 с использованием "устаревших" разговорных терминов (которые описываются в п. 8.1 [b-ITU-T Y-Sup.23]), здесь – столбцы поверхностной проверки пакетов (SPI), средней проверки пакетов (MPI), углубленной проверки заголовков (DHI) и углубленной проверки приложений (DAI).

См. также п. 8 в [b-ITU-T Y.Sup.23] по вопросам применения DPI в многоуровневых архитектурах протоколов.

### 6.2.2 Различия вариантов DPI и вариантов, не относящихся к DPI

Концепция DPI с точки зрения многоуровневых архитектур протоколов довольно обширна и включает даже все уровни протоколов выше уровня 1 (см. п. 3.2.5 [ITU-T Y.2770]). Однако сфера применения проверки пакетов в основном может быть ограничена для конкретного сетевого приложения, например такого, которое зависит главным образом только от линии связи, сети и/или транспортных уровней.

Такое ограничение, как правило, обосновано аспектами, связанными с обслуживанием, традициями и/или реализацией, например компромиссные в экономическом отношении решения, касающиеся достижимых услуг DPI, по сравнению с современными методами. Известен также такой вид ограниченной проверки пакетов, как поверхностная проверка пакетов и средняя проверка пакетов (SPI, MPI; см. также п. 8.1 в [b-ITU-T Y.Sup.23]).

Существенное различие между вариантами DPI и вариантами, не связанными с DPI, в соответствии с [ITU-T Y.2770] является достаточным и также соблюдается в настоящей Рекомендации. Понятие DPI в данном случае (приблизительно) означает правила проверки политики, поддерживаемые в настоящей Рекомендации, а понятие "не относящиеся к DPI" в большей степени относится к проверке пакетов существующими методами на уровнях 2, 3 и/или 4 протоколов (т. е. SPI, MPI).

### 6.2.3 Примеры

В таблице 6-1 приведен список примеров сетевых приложений в сравнении с уровнями проверки пакетов, которые, как правило, являются частью таких сетевых приложений. Следует отметить, что данные приведены в таблице 6-1 лишь в качестве примеров и не всегда являются исчерпывающими.

**Таблица 6-1. Уровень проверки пакетов для некоторых примеров сетевых приложений**

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| **Безопасность** | | | | | | |
| 1.1 | Обнаружение проникновения в сеть | – | X | X | X | Существуют различные методы ID:<br>a) обнаружение аномалий;<br>b) обнаружение неправомерного использования (в данном случае) |
| 1.2 | Обеспечение безопасности сетевых ресурсов (предотвращение проникновения в сеть, предотвращение атак, представляющих угрозу безопасности) | – | X | X | X | |
| 1.3 | Другие функции, связанные с безопасностью | | | | | |

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| **Идентификация** | | | | | | |
| 2.1 | Абонент, пользователь | – | **X** | – | – | Идентифицируется по... ? (например, по сетевому адресу) |
| 2.2 | Тип приложения | – | – | **X** | **X** | Идентифицируется по... ? (например, по типу протокола уровня приложения) |
| 2.3 | Сеанс | – | **X** | – | – | Идентифицируется по... ? (например, по IP-соединению, транспортному IP-соединению). См. также п. 7 в [b-ITU-T Y-Sup.23] |

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| 2.4 | Протокол управления приложениями (например, SIP, RTSP, HTTP, FTP, …) | – | **X** [в зависимости от общеизвестного порта] | **X** | **X** | |
| Характеристики данных в приложениях | | | | | | |
| 2.5 | Контент | – | – | **X** | **X** | Например, нелегальный контент |
| 2.6 | Тип медиаданных (тип данных в приложениях) | – | – | **X** | **X** | |
| 2.7 | Формат медиаданных | – | – | **X** | **X** | |
| **Модификация** (единиц данных протокола) | | | | | | |
| 3.1 | Модификация контента: удаление вирусов | – | – | – | **X** | |
| 3.2 | Модификация заголовка: маркировка QoS | – | **X** | **X** | – | |
| 3.3 | Модификация заголовка и контента: функция ALG | – | **X** | **X** | – | Локальная функция NA(P)T на уровнях L3 (и L4) и уровне приложения |

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| **Контроль параметров использования** | | | | | | |
| 4.1 | Соглашения об уровне обслуживания | – | **X** | **X** | **X** | |
| 4.2 | Контроль параметров трафика<br>Примеры: | – | **X** | **X** | **X** | В зависимости от типа параметра трафика |
| | Ограничение скорости передачи байтов L3 (пиковая скорость, постоянная скорость) | – | **X** | – | – | |
| | Ограничение размера PDU L3 (мин., макс.) | – | **X** | – | – | |
| | Ограничение размера пачки импульсов L3 | – | **X** | – | – | |
| | Ограничение размера SDU L7 (полезная нагрузка приложения) | – | **X** | **X** | – | |
| | Ограничение скорости передачи байтов L7 (объем приложения) | – | **X** | **X** | – | |
| | | | | | | |

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| **Поддержка качества обслуживания** | | | | | | |
| 5.1 | Управление формой трафика | – | **X** | – | – | |
| | Управление скоростью передачи байтов L3 | – | **X** | – | – | См., например, [b-ITU-T Y.1221] или [b-ITU-T H.248.53] |
| | | | | | | |
| **Сетевой анализ** | | | | | | |
| 6.1 | Поведение пользователя | – | **X** | **X** | **X** | |
| 6.2 | Шаблоны использования | – | **X** | **X** | **X** | |
| **Результаты измерения эксплуатационных характеристик (ключевые показатели работы (KPI))** | | | | | | |
| 7.1 | Сбор результатов дистанционных измерений | – | **X** | **X** | **X** | |
| 7.2 | Формирование результатов локальных измерений | – | **X** | **X** | **X** | |
| | | | | | | |

| Сетевое приложение (пример) | | Уровень проверки пакетов | | | | Комментарии |
|---|---|---|---|---|---|---|
| | | Углубленная проверка пакетов (DPI) | | | | |
| | | (Приме-чание) | Углубленная проверка заголовков (DHI) | | Углубленная идентификация приложений (DAI) | |
| | | | Средняя | | | |
| | | | Поверхностная проверка пакетов (SPI) | проверка пакетов (MPI) | | |
| | | Проверка заголовков L2 ($L_2$HI) | Проверка заголовков L3, 4 ($L_{3,4}$HI) | Проверка заголовков L4+ ($L_{4+}$HI) | Проверка полезной нагрузки L7 ($L_7$PI) | |
| **Поддержка начисления платы/выставления счетов** | | | | | | |
| 8.1 | Информация на основе временно́го критерия | – | X | – | – | |
| 8.2 | Информация на основе объема трафика | – | X | – | X | Объем трафика, связанный со скоростью IP-передачи байтов (L3) и/или данными приложений |
| 8.3 | Информация на основе событий | – | X | X | X | В зависимости от типа события (например, событие может быть связано с контентом) |
| | | | | | | |
| **DPI, ориентированная на линию связи** | | | | | | |
| 9.1 | Приложения DPI с возможными условиями политики, относящимися к уровню 2 | X | X | X | X | См. примечание |
| ПРИМЕЧАНИЕ. – Существует принципиальное различие между DPI, ориентированной на линии связи, и DPI, ориентированной на сеть. DPI, ориентированная на линии связи, ограничена сетевым доменом L2, а ориентированная на сеть DPI относится к сигнатурам DPI, которые охватывают протокольную информацию на сетевом уровне (L3) и выше. | | | | | | |

# 7 Структура моделирования

## 7.1 Функциональные модели

Представлено несколько функциональных моделей, иллюстрирующих спектр тракта пересылки пакетов без какой-либо DPI (п. 7.1.2), при однонаправленной DPI (п. 7.1.3) и до модели с двунаправленной DPI (п. 7.1.4).

Все функциональные модели в данном разделе являются примерами таких моделей.

### 7.1.1 Режим "DPI в тракте" по сравнению с режимом "DPI вне тракта"

С точки зрения сквозного тракта передачи пакетов существует два основных сценария развертывания функции узла DPI (DPI-NF):

- DPI в тракте ($DPI_{InP}$) – функция DPI-NF расположена в сквозном тракте передачи пакетов, функция реализации политики (DPI-PEF) выполняет правила политики DPI непосредственно в рамках трафика передачи пакетов (также называется он-лайн-DPI); или
- DPI вне тракта ($DPI_{OoP}$) – функция DPI-NF расположена не в сквозном тракте передачи пакетов, а сосредоточена в пакетной сети, таким образом функция DPI-PEF выполняет правила политики DPI косвенно, например в рамках выборочного трафика передачи пакетов (также называется обходная DPI, оф-лайн-DPI).

Оба режима DPI отличаются с точки зрения физического узла, на котором размещена функция DPI-NF, – функция $DPI_{InP}$ может быть расположена в узле передачи пакетов, а функция $DPI_{OoP}$ будет расположена в узле, *не содержащем* какой-либо функции пересылки пакетов (PFF, см. следующий пункт).

### 7.1.2 Общая пересылка пакетов

Узел передачи пакетов в пакетной сети может быть абстрагирован (на высоком уровне) при помощи функции пересылки пакетов (PFF), как показано на рисунке 7-1. Функция PFF может, например, служить коммутирующей функцией для маршрутизаторов с коммутацией по меткам MPLS (LSR), либо Ethernet-коммутаторов или дополнительных ретрансляторов[2], или функцией пересылки/ маршрутизации для маршрутизаторов IPv4 [IETF RFC 791] и IPv6 [IETF RFC 2460]. Функция PFF должна определять следующий узел (например, следующий участок ретрансляции в сетях на основе IP) для каждого входящего пакета, передаваемого в направлении выхода для одноадресной связи.

Примечание 1. – Многоадресная передача приведет к определению нескольких следующих узлов.

Информация, используемая функцией определения следующего узла (DNNF) для данной функции, хранится в соответствующей базе данных, которая называется базой информации о пересылке (FIB), например таблица пересылки IP MIB в соответствии с [b-IETF RFC 4292] для маршрутизаторов IPv4 согласно определению, приведенному в [b-IETF RFC 1812].

---

[2] ПРИМЕЧАНИЕ. − Таким образом, термин "пакет" (packet) является синонимом термина (L2) "кадр" (frame).

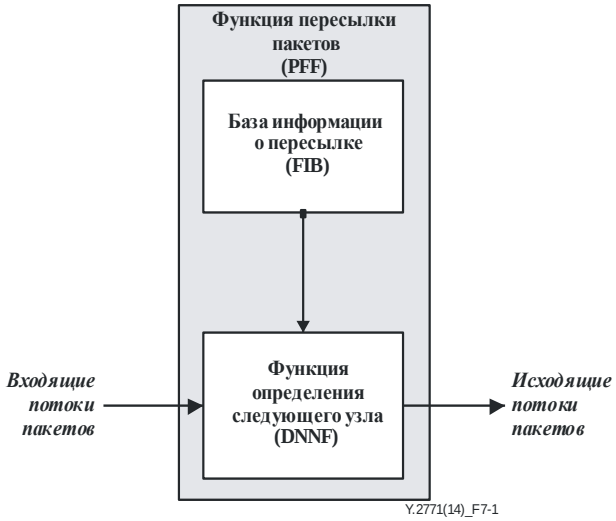



**Рисунок 7-1. Функциональные модели "общая пересылка пакетов"**

Следует отметить, что функция PFF является однонаправленной моделью. Функция DPI (при ее наличии) расположена в тракте передачи пакета (т. е. в режиме DPI в тракте ($DPI_{InP}$)), как правило, перед функцией PFF, см. п. 7.1.3.

Любая подробная информация и требования, касающиеся PFF, не входят в сферу применения настоящей Рекомендации, однако функция PFF отображена в некоторых функциональных моделях для того, чтобы:

- обозначить возможные рабочие характеристики узла DPI при отсутствии какого-либо действующего правила политики DPI (например, временное состояние пустой базы информации о политике DPI (DPI-PIB));
- показать, что конкретные действия в соответствии с политикой, такие как пересылка пакета, все же включают применение функции PFF; и
- создать основу для однозначного определения ряда эксплуатационных показателей, касающихся узлов DPI (см. п. 8).

Следует отметить, что функция PFF может быть неэффективной в том случае, если существует единственный (выходной) тракт передачи пакетов (Примечание 2).

ПРИМЕЧАНИЕ 2. − Пример сценария: узел DPI в тракте, расположенный между двумя узлами передачи пакетов L2 или L3, либо узел DPI в тракте перед пользовательским оборудованием.

### 7.1.3 Однонаправленная DPI

#### 7.1.3.1 Компоненты функции реализации политики однонаправленной DPI

##### 7.1.3.1.1 Общая функциональная модель высокого уровня

На рисунке 7-2 представлена функциональная модель верхнего уровня на основе типовой архитектуры объекта функции DPI (DPI-FE) согласно п. 6.2 [ITU-T Y.2770].

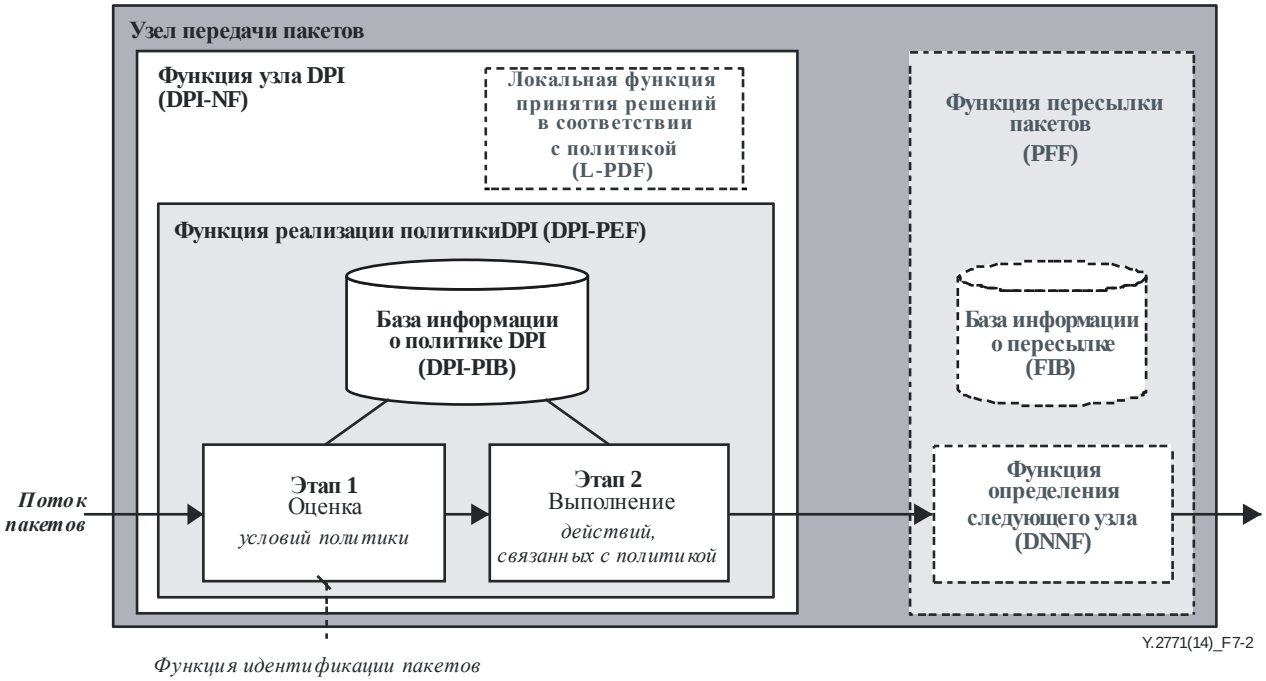



**Рисунок 7-2. Общая функциональная модель высокого уровня**

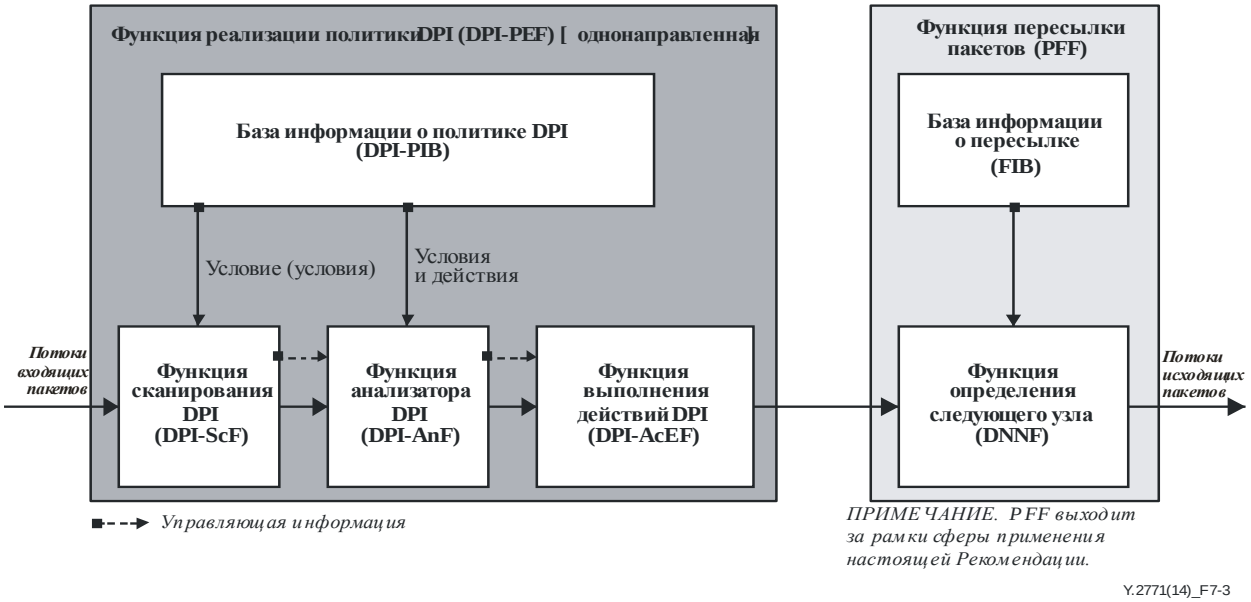
Однонаправленный тракт передачи пакетов моделируется в виде поэтапного процесса. Первый этап представляет функцию идентификации пакетов (см. также п. 7.3.2.1). Эта возможность является важной функцией в контексте DPI и поэтому подробно рассматривается в следующих пунктах (на примерах моделей функционального разложения).

#### 7.1.3.1.2 Основные компоненты в топологии последовательной обработки

На рисунке 7-3 изображен пример однонаправленной модели (в качестве возможной производной от модели верхнего уровня на рисунке 7-2). Функция реализации политики DPI (DPI-PEF) расположена перед функцией PFF – любой входящий пакет сначала обрабатывается функцией DPI-PEF а затем обслуживается функцией PFF. Функция DPI-PEF может быть также организована в функциях тракта передачи пакетов наряду с соответствующей таблицей в качестве хранилища для применяемых правил политики, которое называется базой информации о политике DPI (DPI-PIB) или библиотекой сигнатур DPI. В данном примере обеспечение соблюдения особых правил политики DPI регулируется следующими функциями:

- функцией сканирования DPI (DPI-ScF);
- функцией анализатора DPI (DPI-AnF); и
- функцией выполнения действия DPI (DPI-AcEF).

Данные функциональные компоненты представляются и объясняются в следующем пункте.




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-3. Модели DPI "компоненты функции реализации политики однонаправленной DPI"**

#### 7.1.3.1.3 Дополнительные компоненты

##### 7.1.3.1.3.1 В рамках функции DPI-PEF

Дополнительные компоненты в рамках функции DPI-PEF пока не рассматриваются и подлежат дальнейшему изучению.

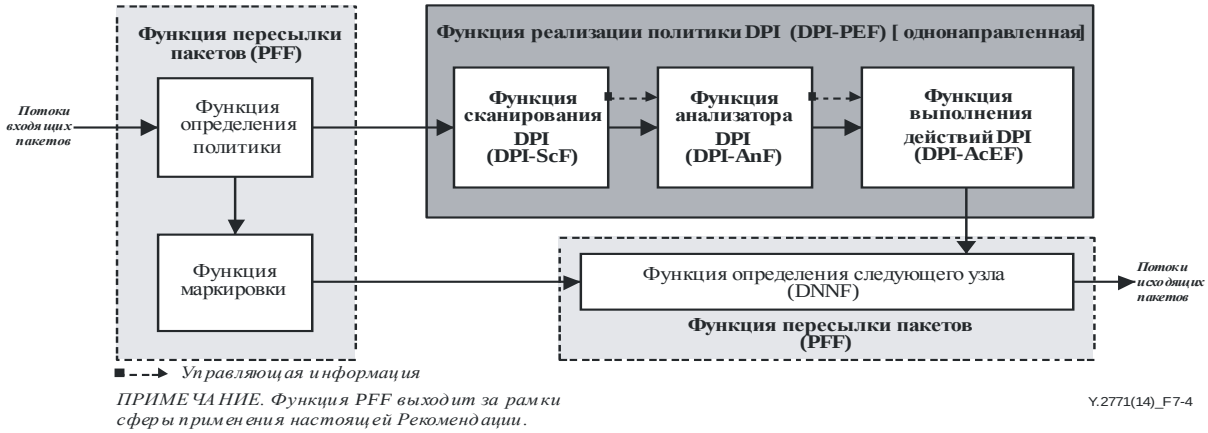
##### 7.1.3.1.3.2 В рамках функции PFF

Функция пересылки пакетов может включать подфункции FE, такие как постановка в очередь, инкапсуляция, формирование, определение политики, маркировка, коммутация, а также DNNF. Однако данные функции не входят в сферу применения настоящей Рекомендации.

#### 7.1.3.1.4 Структурные аспекты тракта обработки пакетов

Вместо последовательного выполнения функций обработки пакетов (как показано на рисунке 7-3) могут также существовать архитектуры узлов DPI с возможностями параллелизма. Например, функция PFF может также обрабатываться параллельно функции DPI-PEF.

На рисунке 7-4 показана модель тракта обработки пакетов с параллельной обработкой пакетов. В данном случае функция определения политики отслеживает пакеты, приходящие в определенный входной порт, или пакеты с заранее определенными критериями (например, специальное условие правил политики), такими как поле IPv4 TOS, отмеченное высоким приоритетом (т. е. правила политики, основанные на SPI). Если эти входящие пакеты или потоки нарушают соглашение о полосе пропускания, то все пакеты или некоторые из них могут быть маркированы соответствующим образом и направлены непосредственно функции DNNF.



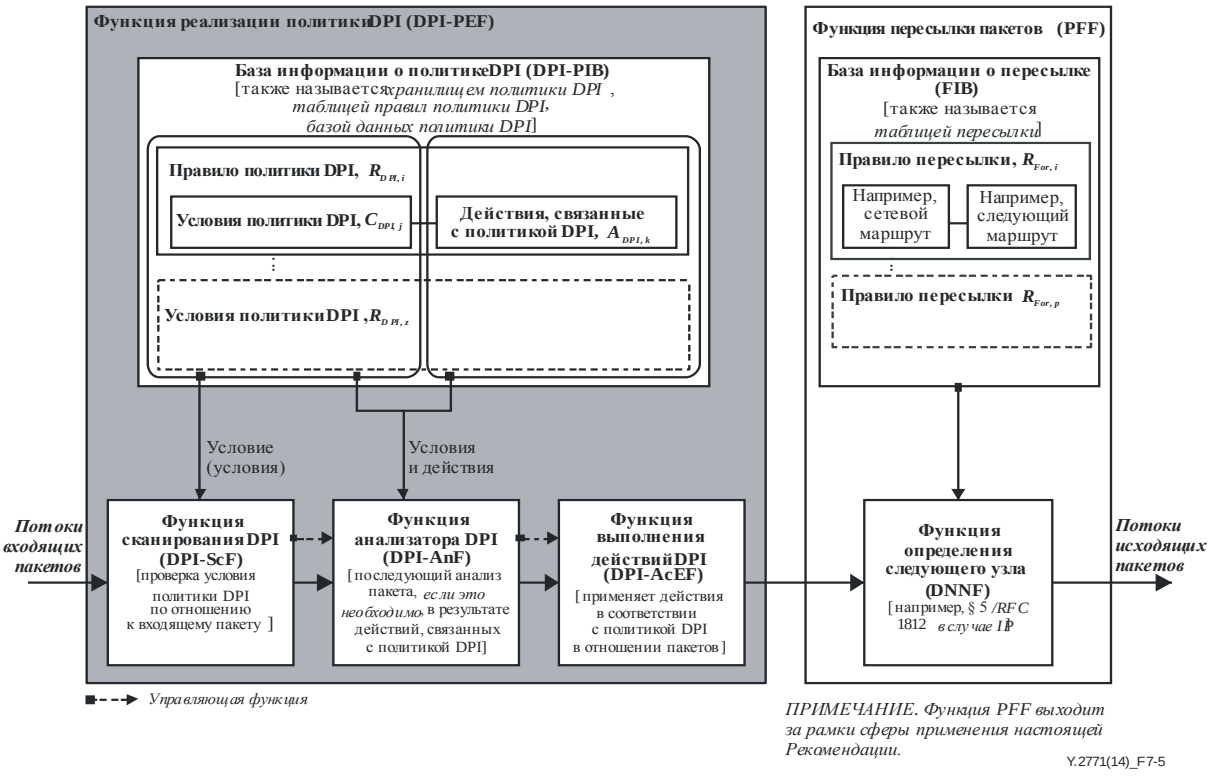

ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.

**Рисунок 7-4. Модель DPI для функции реализации политики однонаправленной DPI с параллельной обработкой пакетов**

Следует отметить, что примеры, приведенные на рисунках 7-3 и 7-4, представляют логические, а не физические топологии. Однако действительная реализация должна отражать тот факт, что тракт обработки пакетов, по которому проходит тот или иной пакет или поток, может отличаться даже в единственном примере DPI.

### 7.1.3.2 Структура базы информации о политике DPI (библиотека сигнатур DPI)

Более детальная структура базы информации о политике DPI представлена на рисунке 7-5, функционально идентичном рисунку 7-3. Правило политики (R) относится к привязке набора действий (A) к набору условий (C). Оценка условий производится для определения того, выполняются ли эти действия. Общеупотребительный термин "правило политики" известен также как (конкретное) правило фильтра для действий, относящихся к функциям фильтрации пакетов (см. также пп. 7.3 и 7.6 в [b-ITU-T Y.Sup.23]).




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-5. Модели DPI "структура базы информации о политике DPI"**

Модель обработки для правил $R_{DPI}$ политики DPI.

1 Функция сканирования DPI (DPI-ScF) проверяет *все* (примечание 1) условия политики DPI, $C_{DPI}$, в отношении входящего пакета.

ПРИМЕЧАНИЕ 1. – Сфера применения того или иного правила политики DPI может охватывать весь трафик передачи пакетов, пересылаемый данным узлом или ограниченный конкретным *потоком* (см. [ITU-T Y.2770]), который определяется дескриптором потока (см. [ITU-T Y.2770]). Поток пакетов может являться, к примеру, объектом сквозного *сеанса* (см. п. 6.7 [ITU-T Y.2770]) между экземплярами приложения (например, для IP-приложений сквозные сеансы могут быть определены как сеансы по HTTP, RTSP, SIP, FTP и т. д.). Реализация правил политики, определяемых сеансом, часто называется определением политики, зависящим от сеанса, в отличие от определения политики, не зависящего от сеанса (это относится к правилам политики для всего совокупного объема трафика, проходящего через узел, в котором реализуется политика). Понятия "поток" и "сеанс" далее в данном пункте подробно не разъясняются, так как не имеют отношения к представленным (высокоуровневым) функциональным моделям.

2 Функция анализа DPI (DPI-AnF) предназначена для дальнейшей проверки условий политики. Функция DPI-AnF работает по принципу конвейера с DPI-ScF, после того как DPI-ScF первоначально отображает каждый пакет (примечание 2). Целью DPI-AnF является улучшение показателей работы.

ПРИМЕЧАНИЕ 2. – Например, функция сканирования может коррелировать входящий пакет с конкретным приложением (например, IP-приложением), а функция анализа может затем провести анализ пакета в зависимости от приложения. Основной принцип, по которому распределяются функции DPI-ScF и DPI-AnF, связан с концепцией последовательной и/или иерархической реализации политики (например, для соответствия показателям качества). Подробности, касающиеся функции DPI-AnF, подлежат дальнейшему изучению.

3 Функция выполнения действия DPI (DPI-AcEF) применяет действия в соответствии с политикой $A_{DPI}$ в отношении сканируемого и анализируемого пакета.

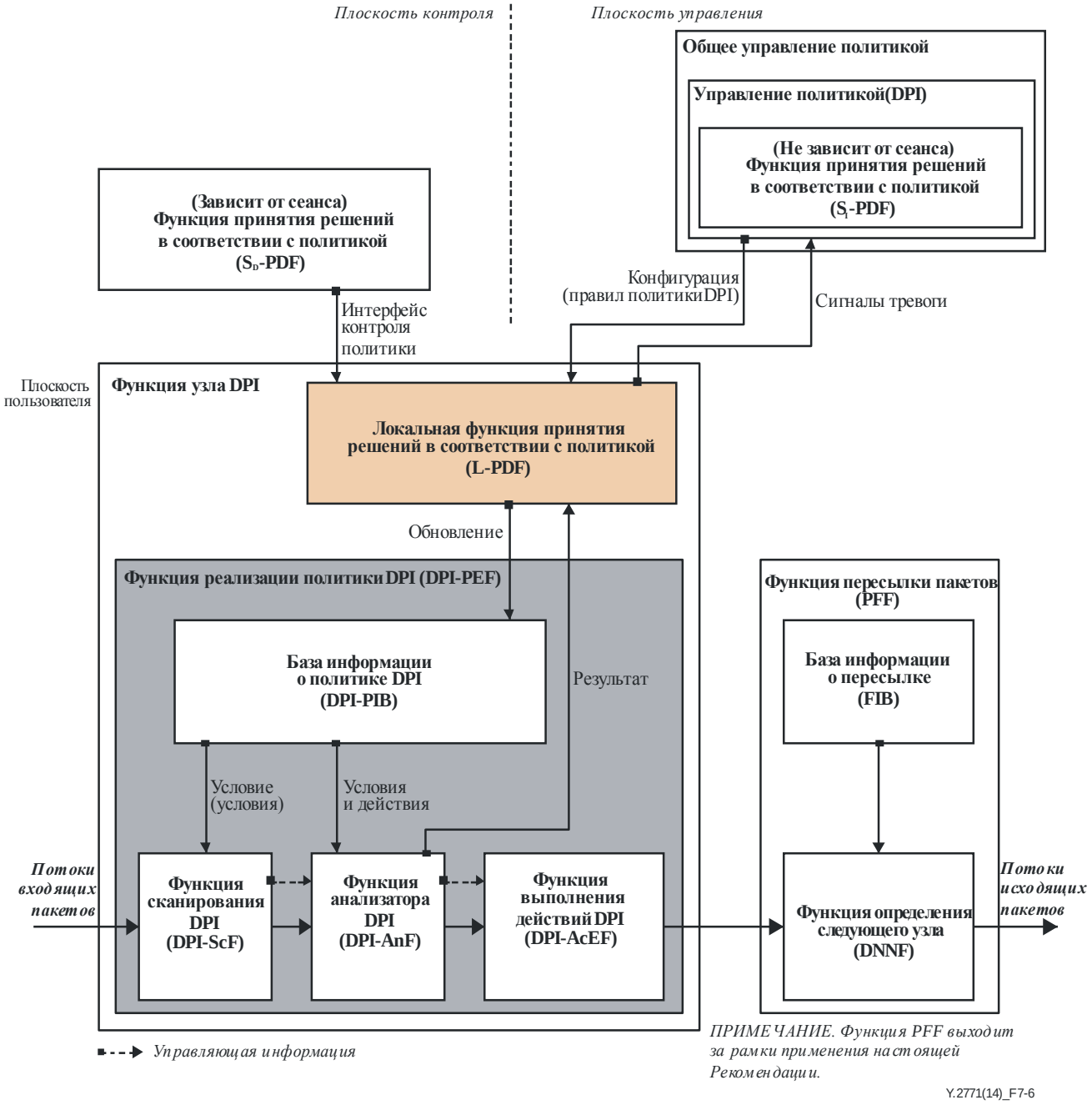
Каждый пакет, который успешно прошел обработку функцией DPI-PEF, будет затем обработан регулярной функций PFF (см. также п. 7.1.2) для режима DPI в тракте.

#### 7.1.3.3 Принятие решений в соответствии с политикой: внесение изменений в базу информации о политике DPI

DPI-PIB предоставляет набор правил политики DPI $R_{DPI,i}$, которые определяют фактические характеристики функции DPI-PEF. Правила политики DPI создаются функциональным объектом принятия решения в соответствии с политикой (DPI-PDFE). На рисунке 7-6 показан пример удаленных функций PDF, расположенных в плоскости контроля и плоскости управления (рисунок 7-7 отображает еще один пример сценария без какого-либо (прямого) доступа из плоскости контроля). Плоскость контроля PDF может отвечать за принятие решений в соответствии с политикой DPI, зависящих от сеанса ($S_D$-PDF). Возможная концепция сеанса упоминается в примечании 1 в п. 7.1.3.2. В [ITU-T H.248.86] приводится определение такого рода интерфейса контроля политики. Плоскость управления PDF может отвечать за принятие решений в соответствии с политикой, не зависящих от сеанса ($S_I$-PDF), см. рисунок 7-6. Управление политикой может главным образом определять правила политики, зависящие и не зависящие от сеанса (как показано в примере на рисунке 7-7).

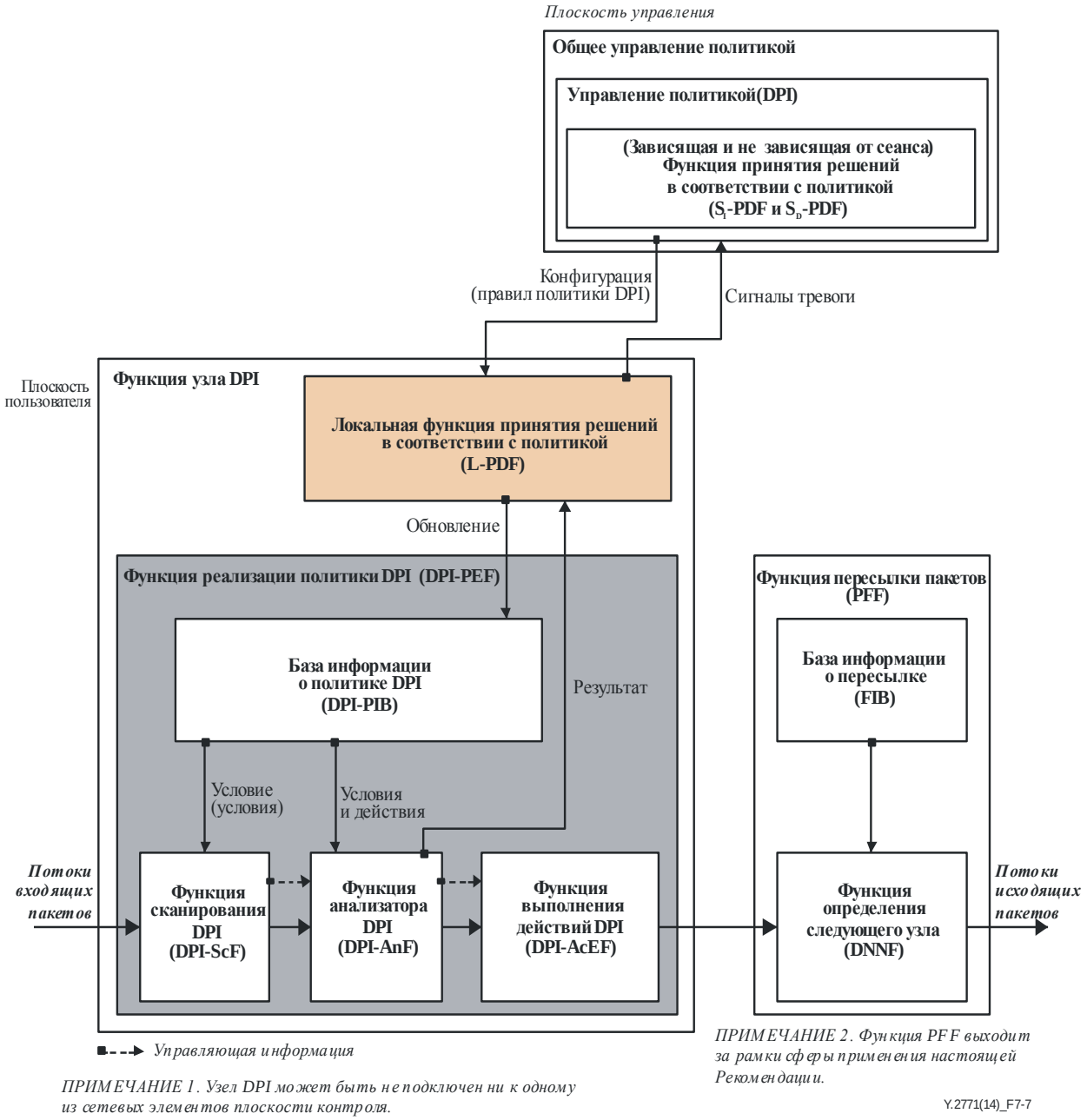
ПРИМЕЧАНИЕ 1. – Определение политики, зависящее от сеанса, может относиться, например, к конкретному приложению, пользователю, типу носителя и т. д., а определение политики, не зависящее от сеанса, может охватывать общие требования безопасности, например ежедневное обновление. Правила политики (DPI) функций $S_D$-PDF и $S_I$-PDF являются взаимодополняющими. На рисунке 7-4 приведен лишь пример конфигурация сети.

Управление политикой DPI, как правило, является частью общего объекта управления политикой, ответственного также за правила политики, не относящиеся к DPI, такие как "существующие" процедуры поверхностной проверки пакетов (SPI) или средней проверки пакетов (MPI).




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-6. Модели DPI "изменение базы информации о политике DPI через плоскости контроля и управления"**




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – Узел DPI может не быть подключенным к какому-либо иному сетевому элементу плоскости контроля.
ПРИМЕЧАНИЕ 3. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-7. Модели DPI "изменение базы информации о политике DPI только через плоскость управления"**

Функции PDF, как правило, расположены в географически удаленных сетевых элементах, как показано на рисунке 7-6 (а также на рисунке 7-7) с помощью интерфейса контроля политики для $S_D$-PDF и интерфейса управления политикой для $S_I$-PDF. Любая удаленная функция PDF может временно находиться в нерабочем состоянии, тем самым приводя в действие дополнительную факультативную локальную функцию PDF (L-PDF) для оптимизации готовности услуги DPI в сети.

L-PDF совместно с DPI-PEF представляет функцию узла DPI.

ПРИМЕЧАНИЕ 2. – Относится к локальному тракту принятия решений в соответствии с политикой на рисунке 7-1 в п. 7.2.1 [ITU-T Y.2770].

Функция L-PDF (если доступна) обеспечивает внешнюю связь с удаленными функциями PDF и внутренний интерфейс с DPI-PEF для обновления DPI-PIB и обработки потенциальных результатов,

полученных от функции анализатора DPI (DPI-AnF). Функция L-PDF может также отвечать за решение потенциальных проблем взаимодействия правил, возникающих между набором правил политики DPI

ПРИМЕЧАНИЕ 3. – Обнаружение и решение проблем взаимодействия правил является основной задачей функций PDF.

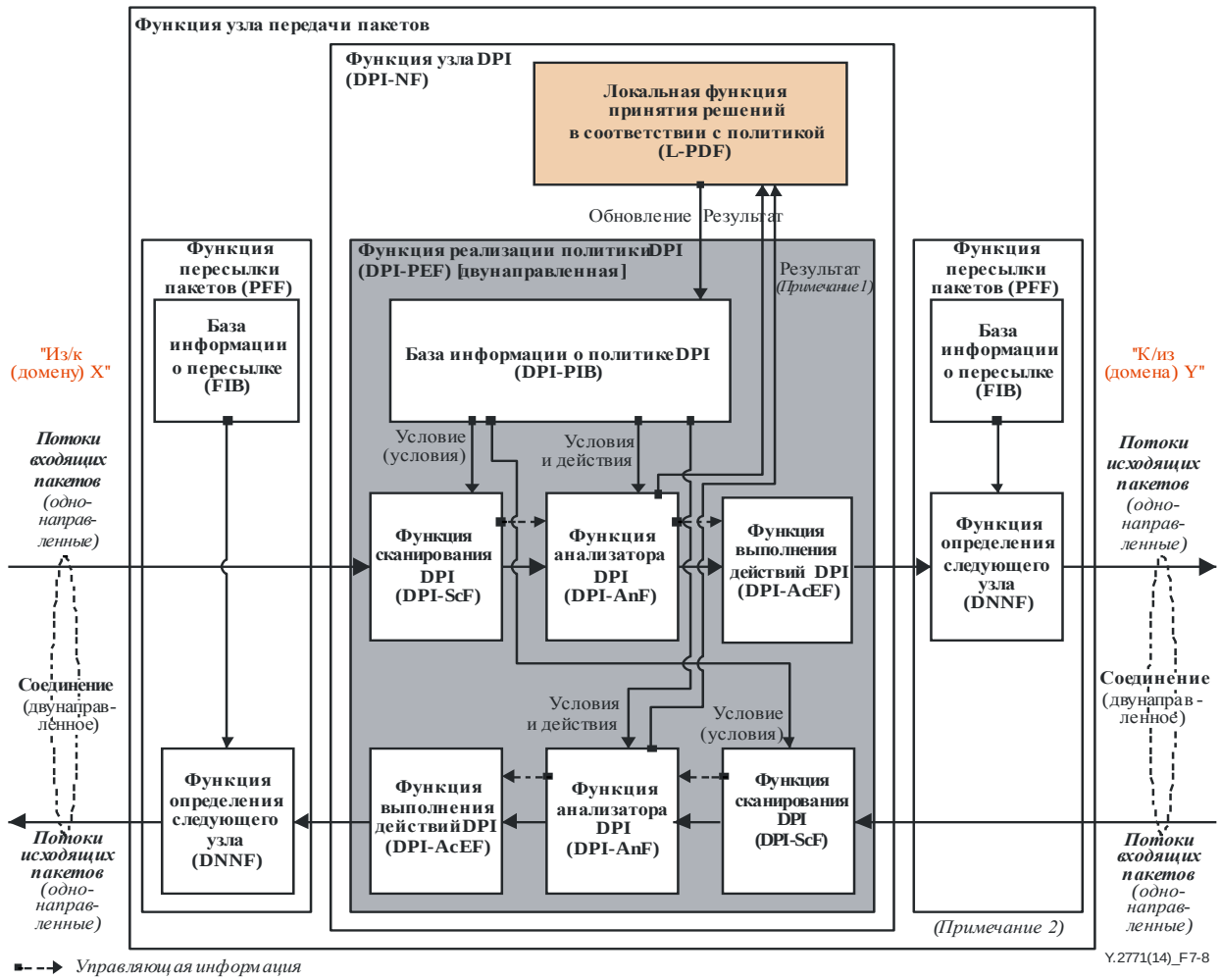
Обратная связь от функции анализатора DPI (DPI-AnF) может привести к отправке сигналов тревоги в адрес функции управления политикой (например, уведомления о новой угрозе безопасности).

Основная модель реализации политики является однонаправленной, но может быть расширена для двунаправленных трактов связи, см. следующий пункт.

### 7.1.4 Двунаправленная DPI

На рисунке 7-8 представлен пример модели двунаправленной DPI (определение которой приведено в п. 3.2.4 в [ITU-T Y.2770]).

Двунаправленное соединение для передачи пакетов состоит из двух однонаправленных потоков пакетов. DPI-PIB является связующим элементом между обоими направлениями трафика с точки зрения реализации политики DPI. Правило политики двунаправленной DPI предоставляет условия политики DPI и/или действия, относящиеся к обоим направлениям трафика.




*ПРИМЕЧАНИЕ 1. DPI-PIB может быть внутренне разделена на базы, зависящие от направления, DPI-PIB, например $DPI_{x \rightarrow y}$–PIB и $DPI_{y \rightarrow x}$–PIB.*

*ПРИМЕЧАНИЕ 2. Функция PFF выходит за рамки сферы применения настоящей Рекомендации.*

ПРИМЕЧАНИЕ 1. – DPI-PIB может быть внутренне разбита на по зависящие от направления базы DPI-PIB, например DPIx ® y-PIB и DPIy ® x-PIB.
ПРИМЕЧАНИЕ 2. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 3. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-8. Модели DPI "двунаправленная DPI"**

Функция L-PDF отвечает за двунаправленную DPI-PEF и предоставляет функцию посредничества путем постобработки возможных результатов, полученных от однонаправленных функций анализатора (DPI-AnF), которые могут затем запускать обновление (местных) правил политики и/или уведомления удаленной функции (функций) PDF.

### 7.1.5 DPI без изменения состояния и DPI с отслеживанием состояния

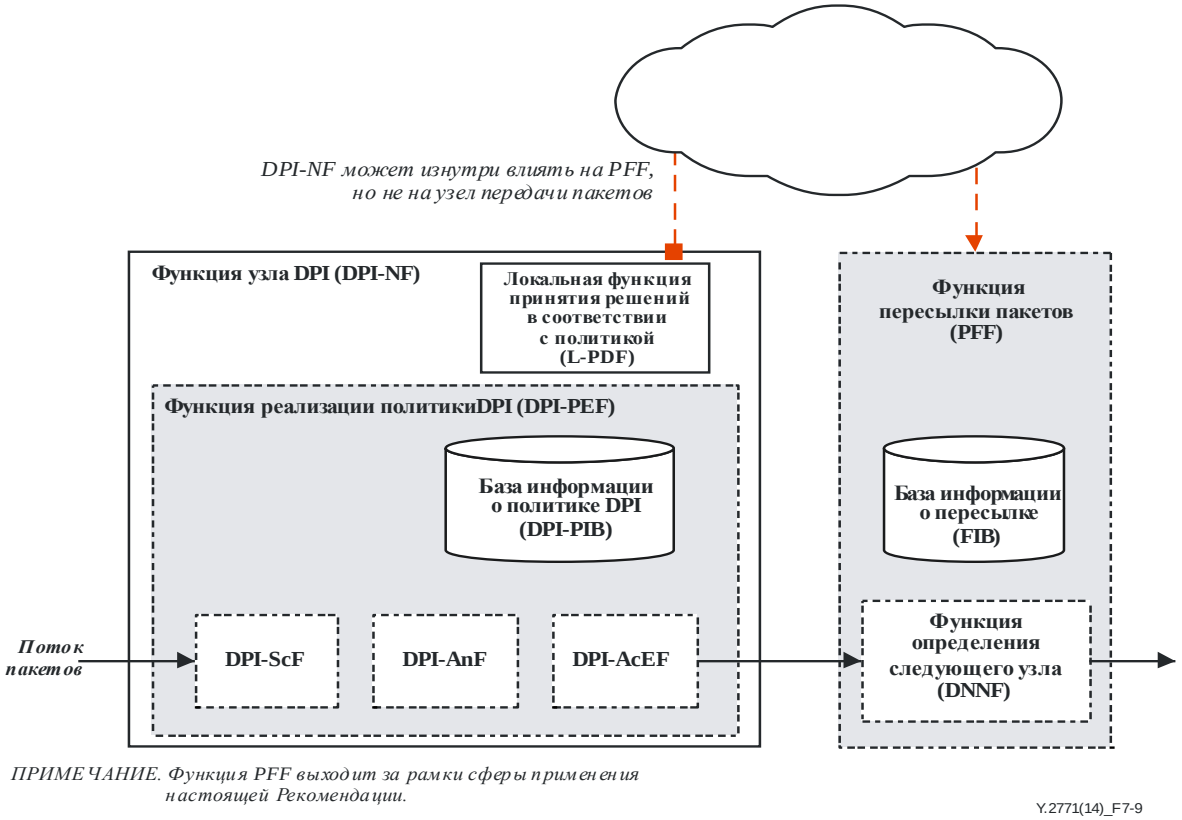
DPI без изменения состояния (технология Stateless DPI) – это правила политики DPI, которые применяются отдельно к каждому пакету, без какой-либо корреляции с другими пакетами однонаправленного потока или двунаправленного соединения для передачи пакетов (см. "условие состояния" в п. 3.2.11 в [ITU-T Y.2770]).

DPI с отслеживанием состояния (технология Statefull DPI) предполагает наличие подобной корреляции (Примечание), которая может быть смоделирована машиной (конечных) состояний. Такая функциональная модель характерна для конкретных правил политики DPI и поэтому не входит в сферу применения настоящей Рекомендации.

ПРИМЕЧАНИЕ. – Например, IP-приложение с транспортировкой данных приложения на базе TCP. Могут существовать одни особые условия политики для этапа установки TCP-соединения, и другие – для последующего этапа активной связи.

### 7.1.6 Влияние DPI на пересылку пакетов

Функция узла DPI может оказывать влияние на следующую за ней функцию пересылки пакетов (PFF) при условии, что PFF доступна или PFF "непустая" (см. п. 7.1.2). Однако функция DPI-NF не должна авторизовываться для локальных модификаций PFF узла передачи пакетов. Скорее она представляет собой вариант, задаваемый внешними удаленными сетевыми элементами узла передачи пакетов (см. рисунок 7-9). Характер конкретного воздействия является предметом принятия решений в соответствии с политикой и/или специальных правил политики DPI и поэтому не входит в сферу применения настоящей Рекомендации.




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – PFF присутствует только для режима DPI в тракте.

**Рисунок 7-9. Возможное влияние DPI на пересылку пакетов через удаленный сетевой объект**

Примеры:

- обновление FIB (информация о сетевом маршруте, см. также рисунок 7-5) с учетом характеристик исследуемой сети, относящихся к сетевой топологии;
- обновление FIB путем блокирования определенных сетевых маршрутов (например, в обратном направлении для двунаправленной DPI).

Следует отметить, что любая локальная модификация PFF, стимулируемая DPI-NF и затребованная внешними сетевыми элементами, должна быть согласована с широкой структурой базовой сети в отношении концепций пересылки пакетов, коммутации и/или маршрутизации (например, определяемых доменом IPv6 DiffServ, доменом MPLS, топологией L2VPN и т. д.).

### 7.1.7 DPI в среде пакетных сетей и сетей СПП

Функция узла DPI встроена в функциональный, физический или виртуальный узел передачи пакетов, который может взаимодействовать с другими функциями в пакетной сети. На рисунке 7-10 представлен пример такой среды. В [ITU-T H.248.86] приведено определение технологии управления DPI, в которой DPI-PDFE и DPI-FE накладываются на модель шлюза, разложенную на составляющие.

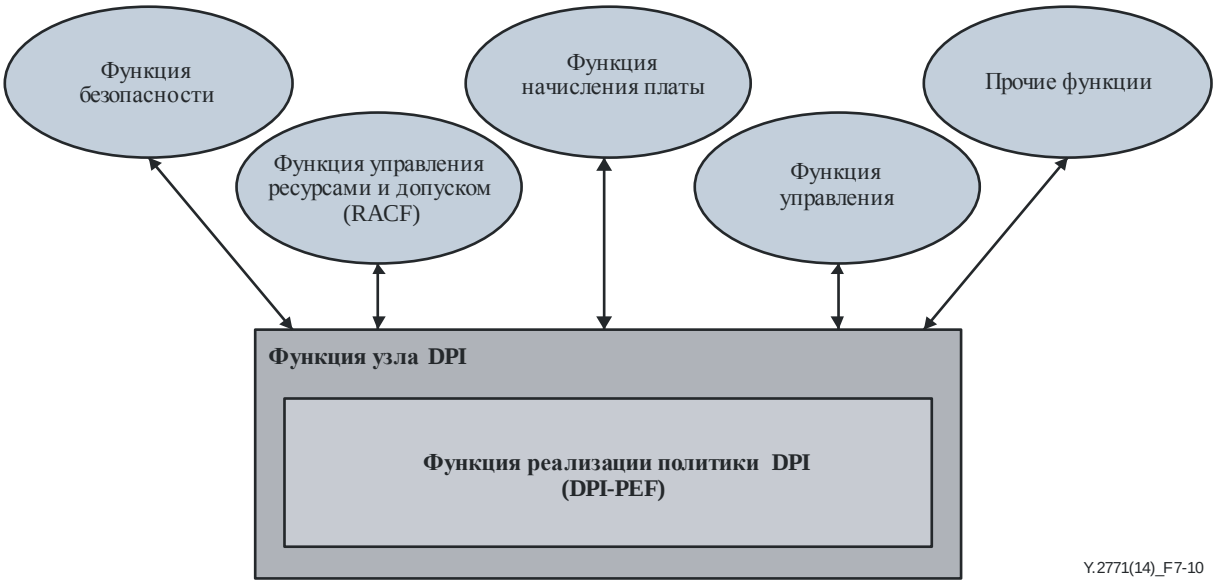



**Рисунок 7-10. DPI в среде пакетных сетей и сетей СПП**

### 7.1.8 Функциональные модели для поддержки измерения потока в рамках группы IETF

#### 7.1.8.1 Характеристика функции измерения потока IPFIX IETF

Определение функции измерения потока IPFIX IETF приводится в [IETF RFC 5101] (см. также п. 6.3.3.2 в [ITU-T Y.2770]). Понятие "поток" относится к потоку пакетов согласно п. 3.1.3 [ITU-T Y.2770], а понятие "измерение" – к измерению метрик эксплуатационных показателей. Следовательно, одна часть функции измерения потока IPFIX содержит условия правил политики для идентификации потока пакетов (на основе идентификатора потоков IPFIX (см. п. 3.2.17 в [ITU-T Y.2770]), а другая относится к действиям на основе правил политики для измерений и действиям по предоставлению отчета.

#### 7.1.8.2 Встроенная функция измерения потока

Процесс передачи потока IPFIX IETF может быть абстрагирован и охарактеризован как правило политики DPI, который таким образом напрямую сопоставлен с DPI-FE. На рисунке 7-11 показана такого рода встроенная функция измерения потока. Отчетность по результатам измерений может передаваться через внешние интерфейсы e2 или e1.

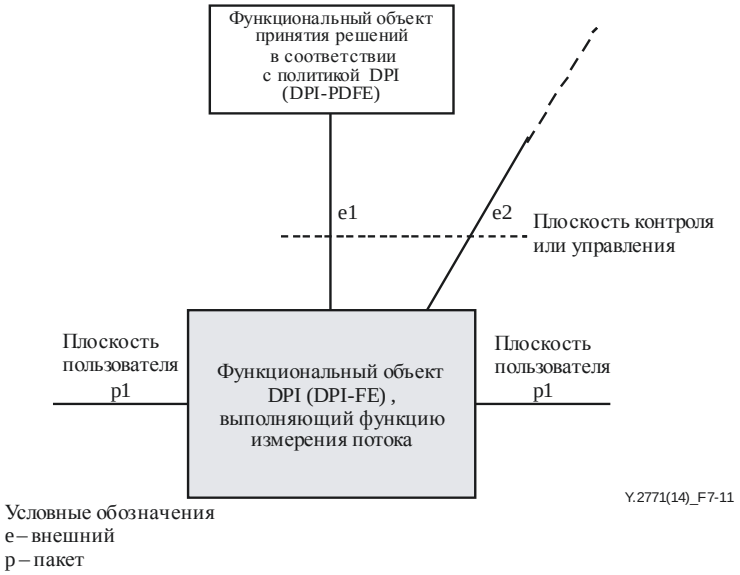



**Рисунок 7-11. Встроенная функция измерения потока**

### 7.1.8.3 Удаленная функция измерения потока

Функция измерения потока может также быть удаленной, т. е. расположенной в тракте передачи пакетов p1, перед или после DPI-FE (см. рисунок 7-12). Конфигурация сети, включающая удаленную функцию измерения потока, может быть задействована, например когда существующая сеть предоставляет физический объект с поддержкой измерения потока, а DPI-PE развертывается дополнительно.

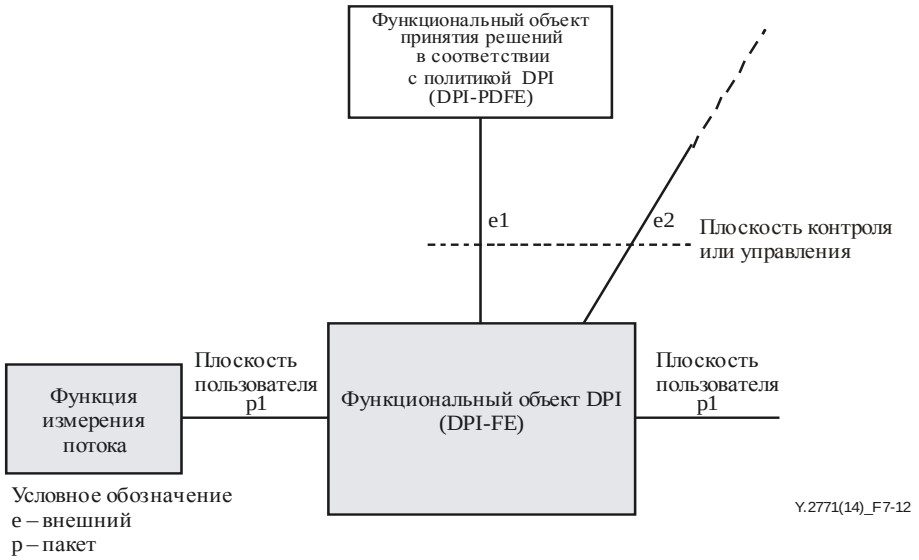



**Рисунок 7-12. Удаленная функция измерения потока**

Объект DPI-FE и удаленная функция измерения потока могут рассматриваться в качестве распределенной архитектуры, имеющей два варианта.

1 Развязанная архитектура – оба функциональных объекта связаны только через p1, следовательно, полностью развязаны в плоскости контроля и управления.

2 Связанная архитектура – например, результаты функции измерения потока можно отправить также через e2 объекта DPI-FE. Такая функциональная модель совместного использования означает наличие нового дополнительного интерфейса (кроме p1) между обоими функциональными объектами.

Сценарии использования для обоих вариантов подлежат дальнейшему изучению.

### 7.1.9 Вероятностная DPI

#### 7.1.9.1 Вероятностная DPI в общем случае

Процесс идентификации пакета может иметь, в сущности, статистический характер (в отличие от детерминированной идентификации пакета), т. е. результат идентификации (в частности критерии соответствия) связан с вероятностью. Такой вид проверки пакета называется вероятностной DPI, а также неопределенной DPI.

Вероятностная DPI соответствует правилам политики DPI, условия которых могут быть, например, следующими.

− Набор $S$ сигнатур содержит сигнатуры $S_1$, $S_2$ …, $S_N$. Набор $S$ сигнатур представляет составные условия политики согласно булевой дизъюнктивной нормальной форме (DNF), т. е. сигнатуры $S_i$ ($i$ = 1, 2…$N$) объединяются в виде списка на основе OR. Два этапа DPI имеют следующие характеристики: 1-й этап – выработка условий политики основана на вероятностном процессе; и 2-й этап – выполнение условий политики приводит к детерминированным результатам соответствия, таким образом приводя в целом к вероятностной DPI.

Основной целью вероятностной DPI является быстрое и эффективное определение того, соответствует ли пакет набору сигнатур $S$. Конкретная информация о соответствии, т. е. какая именно сигнатура $S_i$ была определена, является второстепенной. Набор $S$ сигнатур в общем случае представляет вариант идентификации для определенного приложения. Тег связанного приложения, например "пакет с сигнатурой в наборе $S$", может быть предметом отчетности.

#### 7.1.9.2 Вероятностная DPI на основе фильтра Блума

DPI на основе фильтра Блума является общеизвестным представителем вероятностной DPI, обусловленной характерным коэффициентом ошибок $\varepsilon_{DPI}$ с точки зрения ложноположительных срабатываний $\varepsilon_{f-p}$ (см. п. 8.2.3.3.1), базового подхода к проверке пакетов.

Пример конкретного приложения, реализованного в виде фильтра Блума.

− DPI применяется для обнаружения "трафика приложения x". Трафик приложения x характеризуется набором сигнатур: $S$ = {application x v1, application x v2…, application x vk}, т. е. отдельных сигнатур, относящихся к характеристикам, зависящим от приложения. В таком случае может существовать пример правила политики DPI для определения того, содержит ли пакет "приложение x" при помощи вышеуказанного набор сигнатур в качестве составного условия правил политики DPI, и исключения пакета при наличии соответствия, при этом конкретная версия приложения x не имеет значения.

  Основная причина использования вероятностной DPI на основе фильтра Блума – своего рода компромисс между точностью идентификации и ресурсоемкостью идентификации (например, с точки зрения процессорного времени и/или памяти). Подобный подход позволяет существенно упростить обработку DPI.

DPI на основе вероятностной характеристики фильтра Блума задается следующим процессом.

− Любой полученный пакет $P$ сравнивается с фильтром Блума, представляющим собой полный набор $S$ сигнатур одновременно; если пакет $P$ соответствует одной или нескольким сигнатурам набора $S$, то результат будет соответствовать достоверности вероятности предполагаемой информации $P_{Hit,\ BloomFilter,\ S}$, в соответствии с уравнением

$$P_{Hit,\ BloomFilter,\ S} = 1 - \varepsilon_{f-p} = 1 - \left(1 - e^{-kN/m}\right)^k \tag{7-1}$$

со значениями параметров:

$m$ – размер фильтра Блума в битах;

$N$ – количество сигнатур в наборе $S$;

$k$ – количество хэш-функций, используемых для создания фильтра Блума.

Понятие "вероятностный" относится к "точности идентификации" DPI-FE, касающейся идентификации пакета, потока, приложения и т. д., и тесно связано с метриками рабочих характеристик области коэффициентов ошибок (см. п. 8.2). Информация о вероятностной DPI, реализованной при

помощи фильтров Блума, приведена в Дополнении I, эксплуатационный показатель коэффициент ложноположительных ошибок (DPI) $\varepsilon_{f\_p}$ и эксплуатационный показатель коэффициент ложноотрицательных ошибок (DPI) $\varepsilon_{f-n}$ равны нулю.

## 7.2 Информационные модели и модели данных

Процесс поэтапного развития услуг связи [b-ITU-T I.130] различает уровни абстракции "информации" и "данных" (такие как единицы данных, касающихся протоколов). Информационные модели используются на очень высоком уровне в целях описания, например, потока информации между сетевыми объектами (см., например, [b-ITU-T I.130], [b-ITU-T X.1036]). Модели данных расположены на более низком уровне, например для описания элемента информации с синтаксической точки зрения (см., например, [b-ITU-T J.380.1]).

### 7.2.1 Информационная модель (пример структуры)

Любой вид подробной спецификации для моделирования информации и информационных потоков, касающихся правил политики DPI, выходит за рамки сферы применения Рекомендаций "структурного" типа. Однако моделирование информации о правилах политики DPI может служить примером основы [b-IETF RFC 3060]. В таблице 7-1 отображено несколько примеров элементов информации в целях предоставления некоторых руководящих указаний (на предмет того, каким образом может быть разработана конкретная модель).

**Таблица 7-1. Пример информационной модели, основанной на [b-IETF RFC 3060]**

| Элемент информации (настоящая Рекомендация и [ITU-T Y.2770]) | Общая базовая информационная модель политики в соответствии с [b-IETF RFC 3060] |
|---|---|
| Правило политики DPI | Может быть основано на классе "PolicyRule" |
| Условие (составное) правила политики DPI | Может быть основано на абстрактном классе "PolicyCondition" |
| Условие (единичное) правила политики DPI | Может быть основано на абстрактном классе "PolicyCondition" |
| Действие в соответствии с правилами политики DPI | Может быть основано на абстрактном классе "PolicyAction" |
| И так далее, например, группирование и пиритизация правил политики DPI, характеристик, в частности срока действия правил и т. д. | … |

### 7.2.2 Модель данных (пример структуры)

Любой вид подробной спецификации для моделирования объектов данных, относящихся к правилам политики DPI, выходит за рамки сферы применения Рекомендаций "структурного" типа (поскольку, вероятно, в таком случае будет открыта область разработки синтаксиса протокола).

Однако моделирование информации о правилах политики DPI может служить примером основы [b-IETF RFC 4011]. В таблице 7-2 отображен ряд примеров объектов данных в целях предоставления некоторых руководящих указаний (на предмет того, каким образом может быть разработана конкретная модель).

**Таблица 7-2. Пример модели данных, основанной на [b-IETF RFC 4011]**

| Элемент информации (настоящая Рекомендация и [ITU-T Y.2770]) | Общий объект данных, использующий MIB управления на основе политики согласно [b-IETF RFC 4011], приведен в качестве примера |
|---|---|
| DPI-PIB | Может быть основана на объекте "pmPolicyTable", который и в этом случае связан с объектом "pmPolicyCodeTable" (Примечание 1) |
| Правило политики DPI, т. е. запись DPI-PIB | Может быть основано на объекте "pmPolicyEntry" |
| Условие правила политики DPI | Может быть основано на объекте "pmPolicyCodeEntry" (Примечание 2) |
| Действие в соответствии с правилами политики DPI | Может быть основано на объекте "pmPolicyCodeEntry" (Примечание 2) |
| и т. д. | и т. д. |
| ПРИМЕЧАНИЕ 1. – Абстракция и разделение "описания правила" и "кода правила" на две связанные таблицы дает возможность определить эффективную DPI-PIB.<br>ПРИМЕЧАНИЕ 2. – То есть условие правил и действие в соответствии с правилами могли бы в конечном счете использовать ту же модель объекта данных (в этом примере). | |

С точки зрения сетевой плоскости следует отметить, что общий *объект данных* может быть виден как:

- управляемый объект с точки зрения плоскости управления DPI (см. интерфейс *e2* в п. 8 [ITU-T Y.2770]); и/или как
- контролируемый объект с точки зрения плоскости контроля DPI (см. интерфейс *e1* в п. 8 [ITU-T Y.2770]).

Например, DPI PD-FE может (через e1) сигнализировать об определенном правиле политики DPI либо это правило может быть предоставлено (через e2) системой управления DPI, но результатом является одна и та же запись объекта данных – "правило политики DPI" в DPI-PIB.

## 7.3 Модели трафика

### 7.3.1 Введение

Целью данного раздела является описание ряда представляющих интерес характеристик объектов DPI (определение см. в п. 3.2.7 в [ITU-T Y.2770]) с точки зрения теории трафика. Полученные аспекты могут способствовать последующему определению, например, функциональных, эксплуатационных требований и требований готовности, отображению архитектурных аспектов или оценки эксплуатационных характеристик.

Описанные модели трафика являются лишь примерами и не всегда представляют конкретные компоненты DPI (такие как DPI-PE, DPI-FE, ядро DPI, библиотека сигнатур DPI и т. д.).

### 7.3.2 Базовые модели трафика для обработки в тракте передачи пакетов

Обработка трафика производится на уровне детализации пакетов, основных функций DPI-FE, и выполняется главным образом встроенным ядром DPI (определение см. в п. 3.2.6 в [ITU-T Y.2770]).

Ядро DPI является базовым компонентом DPI-FE и играет важную роль в DPI-FE. Трафик DPI обрабатывается ядром DPI. Когда ядро DPI будет реализовано как физический компонент, параллельная обработка может способствовать улучшению эксплуатационных показателей ядра DPI. Следовательно, может существовать несколько обрабатывающих модулей в рамках физического компонента, соответствующего ядру DPI.

#### 7.3.2.1 Базовая модель трафика DPI-FE с областью действий ядра DPI

На рисунке 7-13 использован пример функциональной модели DPI-FE в соответствии с рисунком 6-1/[ITU-T Y.2770] для получения типовой модели трафика. Модель трафика нацелена только на тракт передачи пакетов, предоставляя тем самым модель для ядра DPI.

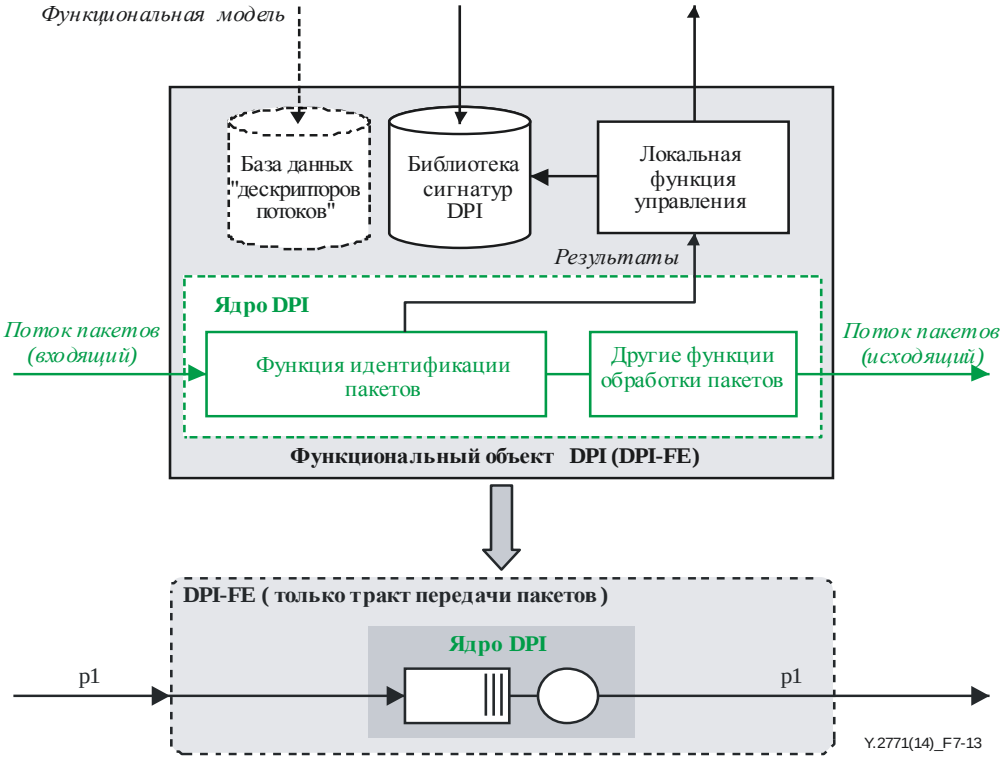



**Рисунок 7-13. Базовая модель трафика DPI-FE с областью действий ядра DPI**

Эта модель характеризуется наличием единственного сервера и конечной очереди ожидания. Следовательно, сервер обрабатывает все функции тракта передачи пакетов. Одноступенчатая модель сервера представляет модель трафика для однонаправленного потока пакетов.

### 7.3.2.2 Ядро DPI: расширение до обработки многоступенчатого тракта передачи пакетов

#### 7.3.2.2.1 Ядро DPI на базе двухступенчатого сервера

На рисунке 7-14 представлен пример двухступенчатой модели трафика ядра DPI.

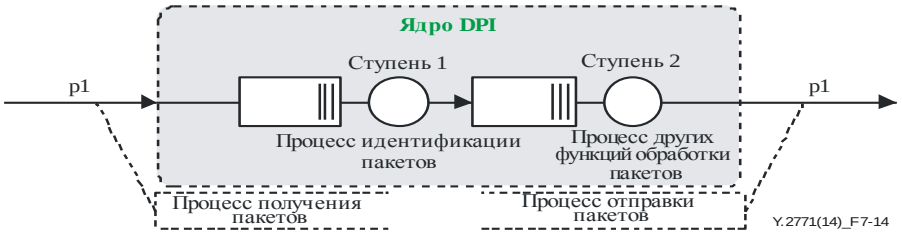



**Рисунок 7-14. Модель трафика ядра DPI: расширение до двухступенчатого тракта передачи пакетов**

В данном примере первый сервер отвечает за обработку условий правил DPI.

#### 7.3.2.2.2 Ядро DPI на базе трехступенчатого сервера

Ядро DPI внутренне может быть реализовано как распределенная система, например как серия последовательно соединенных обрабатывающих элементов. Например, образец функциональной модели согласно рисунку 7-3 представляет три этапа обработки, которые называются сканирование DPI, анализ DPI и выполнение действий DPI – сокращенно DPI-ScF, DPI-AnF и DPI-AcEF, соответственно.

На рисунке 7-15 представлен пример соответствующей модели трафика.

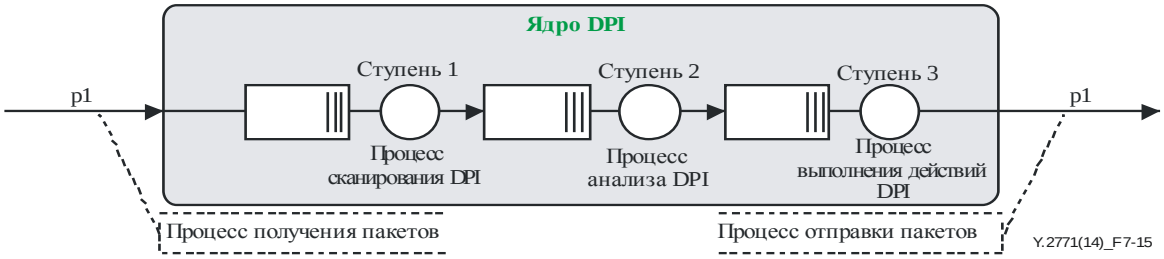



**Рисунок 7-15. Модель трафика ядра DPI: расширение до трехступенчатого тракта передачи пакетов**

### 7.3.3 Расширенные модели трафика для ядер DPI

#### 7.3.3.1 Единый внешний интерфейс и внутренний параллелизм

Пример: может существовать объект DPI вне тракта (см. п. 6.1), который через единый сетевой маршрут подключен к пакетной сети. Целью такого объекта DPI может являться оф-лайн-обработка большого количества выбранных потоков пакетов, т. е. может потребоваться высокая производительности обработки. Параллелизм может быть одним из вариантов достижения высокой производительности обработки. На рисунке 7-16 представлен пример модели трафика на уровне нескольких параллельных ядер DPI.

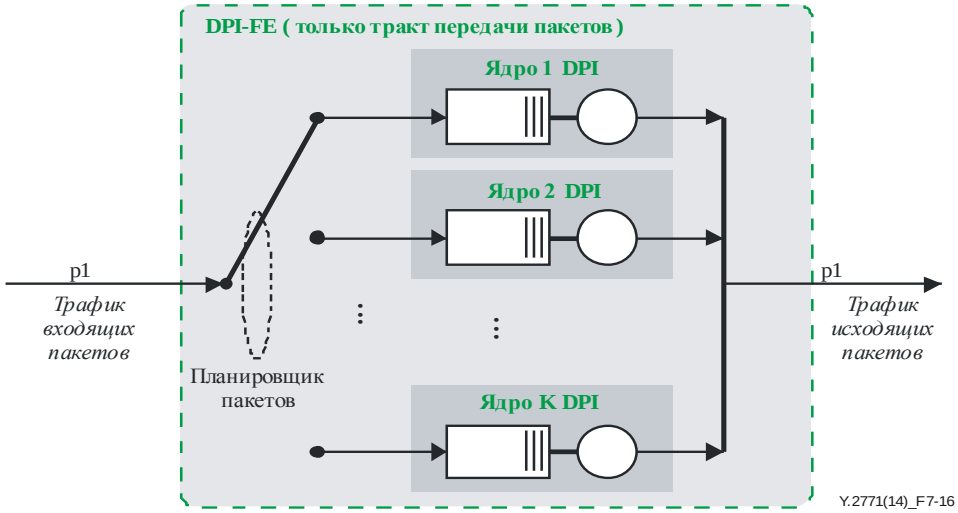



**Рисунок 7-16. Ядра DPI – единый внешний интерфейс и внутренний параллелизм**

Эта модель трафика подразумевает функцию планировщика пакетов для распределения входящего пакета в адрес ядра (сервера) DPI. Подобная функция выходит за рамки сферы применения настоящей Рекомендации.

ПРИМЕЧАНИЕ. – Например, планировщиком пакетов может являться:

a) простой алгоритм распределения нагрузки (т. е. планирование, основанное только на предполагаемом состоянии загрузки серверов ядра DPI), единственный, который действительно имеет смысл для DPI без изменения состояния;

b) информация, основанная на дескрипторе потока (для рассмотрения варианта DPI с отслеживанием состояния), но тогда должна существовать как минимум двухступенчатая модель сервера с точки зрения моделирования трафика; или

c) другие виды методики планирования.

#### 7.3.3.2 Несколько внешних интерфейсов и внутренний параллелизм

Объект DPI в тракте, расположенный на уровне ядра сети (см. п. 6.1), в основном предоставляет несколько физических интерфейсов p1. Несколько ядер DPI могут параллельно обслуживать все входящие потоки пакетов (см. рисунок 7-17). Как правило, существует требование, согласно которому все ядра DPI (т. е. *K*) должны подключаться ко *всем* интерфейсам входящих пакетов p1 (например, *N*).

Таким образом, для данной цели потребуется функция коммутирующей матрицы пакетов *N–K*. Подобная функция выходит за рамки сферы применения настоящей Рекомендации.

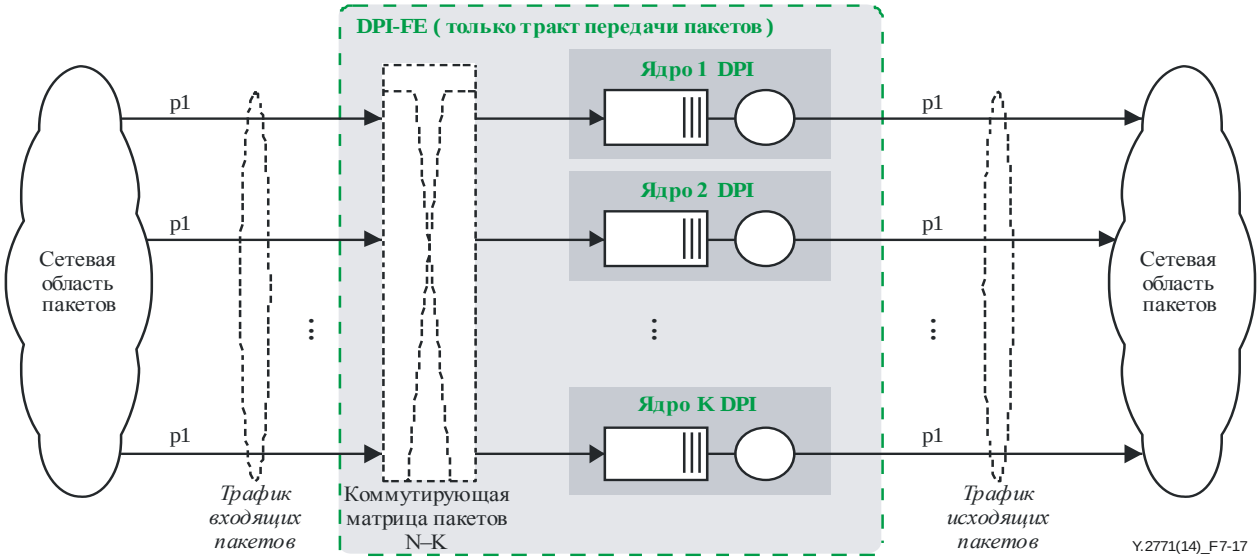



**Рисунок 7-17. Несколько внешних интерфейсов и внутренний параллелизм**

### 7.3.3.3 Параллельные ядра DPI на базе трехступенчатых серверных моделей

На рисунках 7-18 и 7-19 показана расширенная модель, основанная на сочетании моделей трехступенчатого ядра DPI (п. 7.3.2.2.2) и параллелизма на уровне ядер DPI (п. 7.3.3.1).

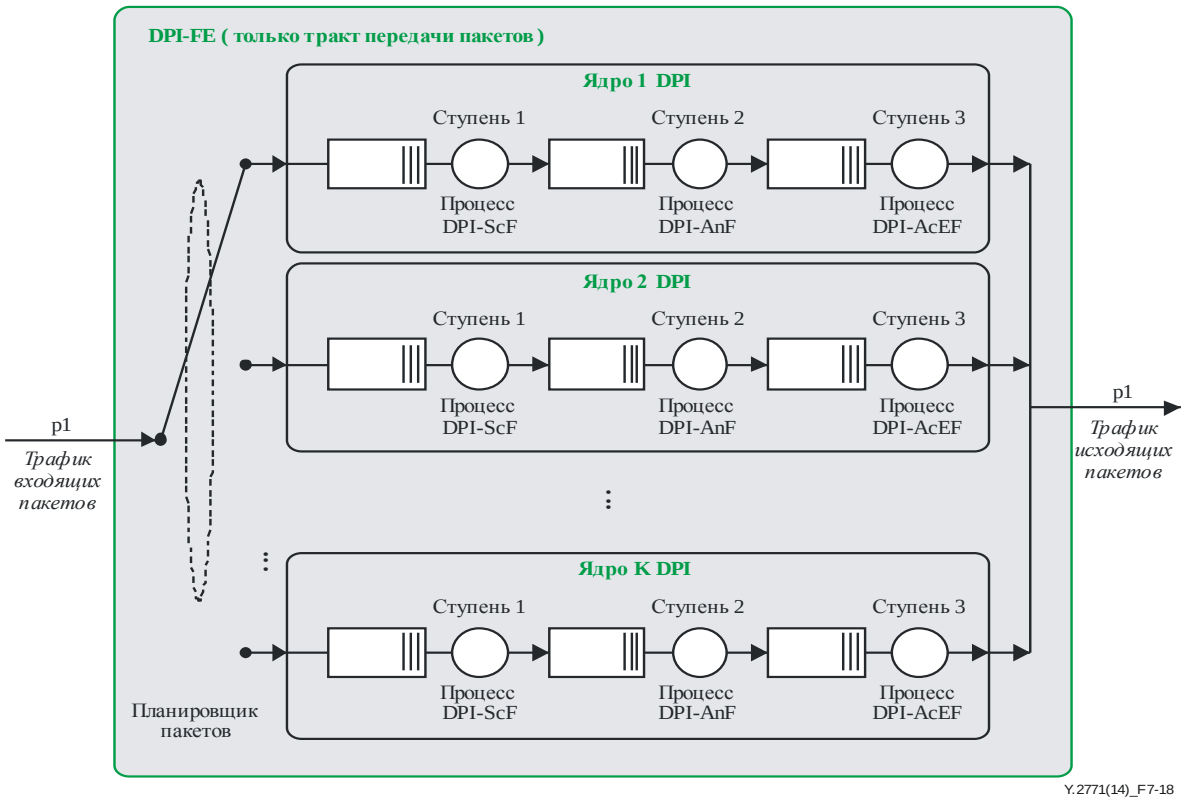



**Рисунок 7-18. Параллельные ядра DPI на базе трехступенчатых моделей серверов (единый внешний интерфейс)**

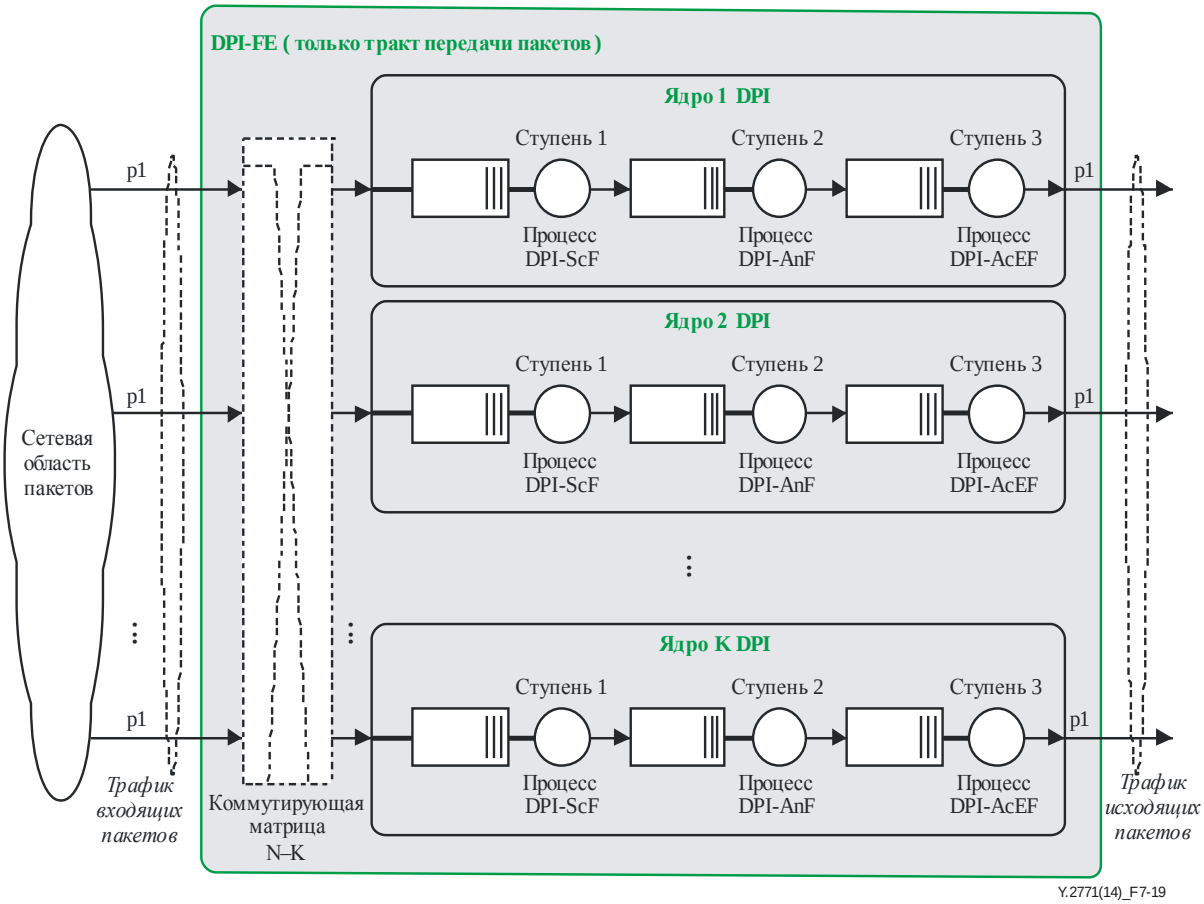



**Рисунок 7-19. Параллельные ядра DPI на базе трехступенчатых моделей серверов (несколько внешних интерфейсов)**

Модели трафика характеризуются параллельными ядрами DPI, работающими абсолютно одновременно, т. е. между ядрами DPI отсутствуют зависимости. Максимальная производительность подобной архитектуры DPI-PE может быть достигнута в том случае, если загрузка всех серверов будет оптимальной (т. е. ни один сервер не перегружен или недогружен), что подразумевает равномерное распределение нагрузки в обоих измерениях модели трафика. Проектирование подобной архитектуры является достаточно сложной задачей, решение которой, вероятно, возможно лишь для некоторых конкретных вариантов распределения трафика, относящихся к предлагаемой загрузке пакетов.

Такого рода ситуация может привести к возникновению различных архитектур, подобных тем, которые рассматриваются в следующем пункте.

#### 7.3.3.4 Единое ядро DPI на базе трех ступеней и внутреннего параллелизма

На рисунках 7-20 и 7-21 представлен пример единого ядра DPI, основанного на трех ступенях обработки и наличии параллелизма на каждой из ступеней. Уровень параллелизма может отличаться в зависимости от ступени, т. е. на разных ступенях может существовать различное число серверов (т. е. различные значения $K_1$, $K_2$ и $K_3$).

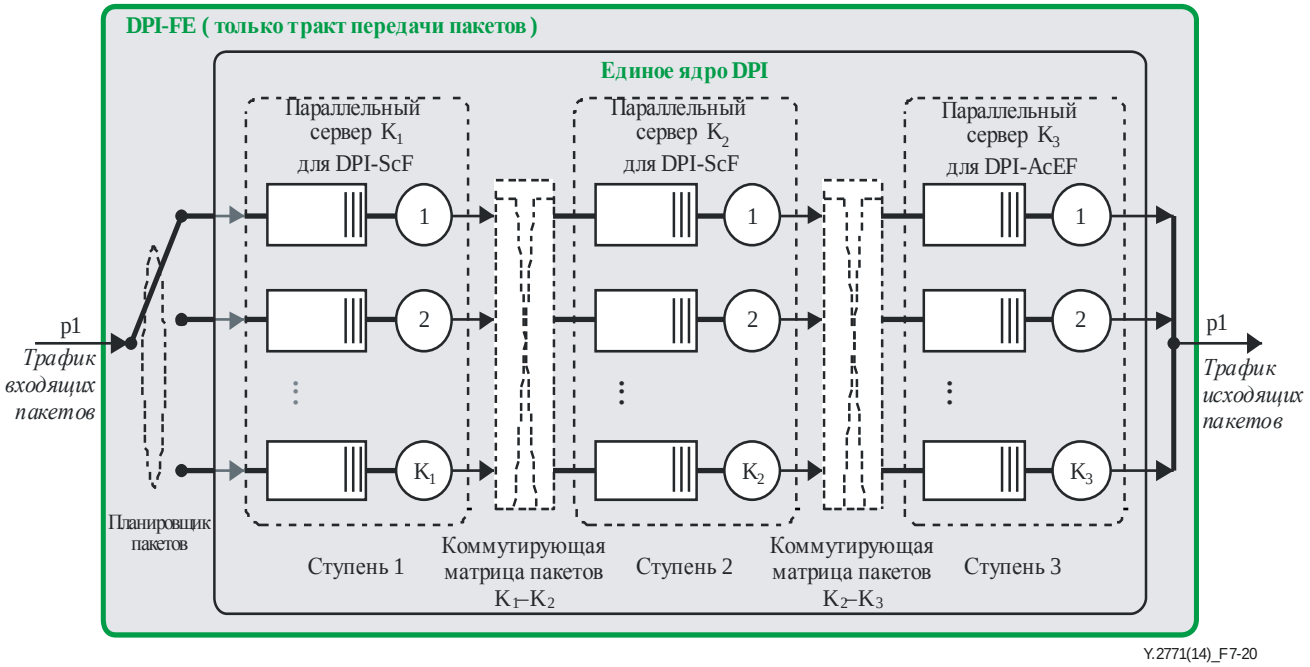



**Рисунок 7-20. Единое ядро DPI на базе трех ступеней и внутреннего параллелизма (единый внешний интерфейс)**

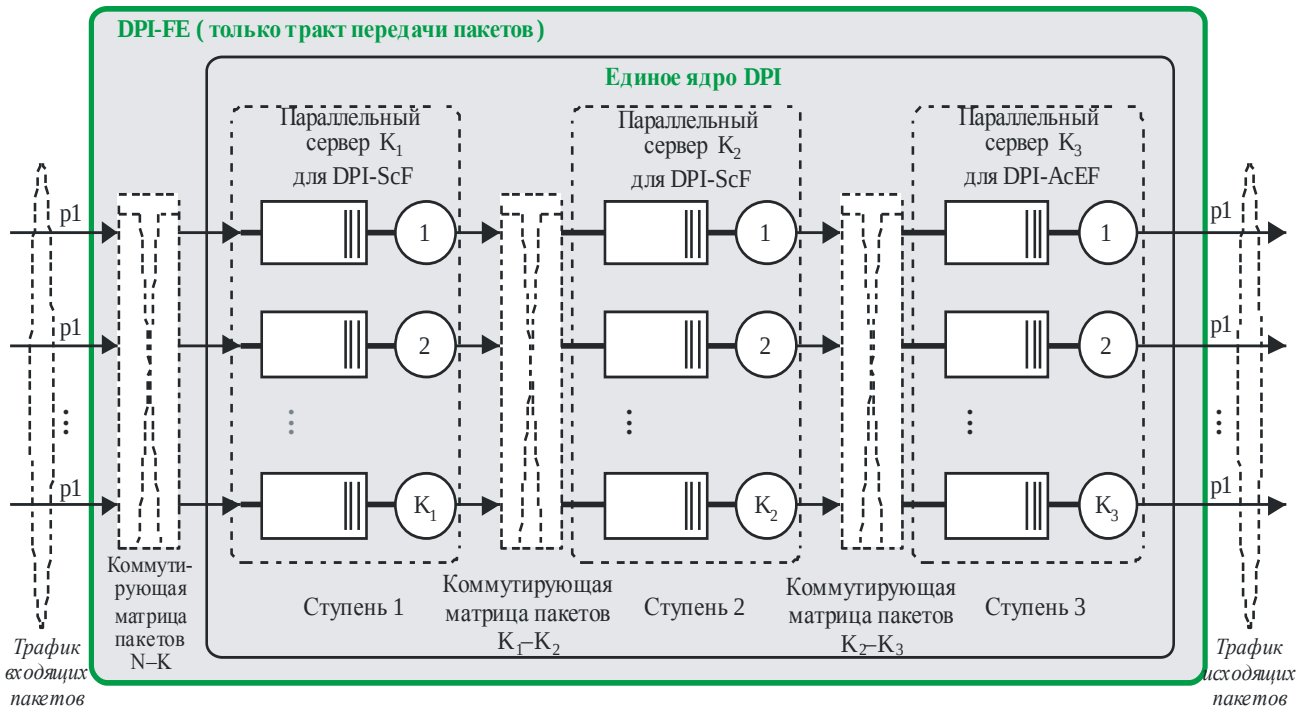



**Рисунок 7-21. Единое ядро DPI на базе трех ступеней и внутреннего параллелизма (несколько внешних интерфейсов)**

Если ядро DPI должно поддерживать режим DPI с отслеживанием состояния, то может потребоваться маршрутизация *всех* пакетов *и того же потока* по тому же тракту серверов в связи с наличием локальной информации о состоянии. Данный аспект выходит за рамки сферы применения вышеуказанной модели трафика.

## 7.4 Идентификация возможных субкомпонентов DPI-FE

Объект DPI-FE может быть разделен на функциональные субкомпоненты, как уже показано на примерах функциональных моделей в предыдущих пунктах. В таблице 7-3 представлен обзор типовых функциональных субкомпонентов в рамках DPI-FE. Эти компоненты частично упоминаются в последующих пунктах (например, при обсуждении аспектов производительности, возможных функциональных или эксплуатационных требований и т. д.).

**Таблица 7-3. Типовые субкомпоненты DPI-FE**

| Компонент | Описание |
|---|---|
| Функция реализации политики DPI (DPI-PEF) | Функциональный элемент, относящийся к реализации правил политики DPI, который содержит как минимум базу информации о политике DPI, функцию идентификации пакетов DPI и функцию выполнения действий DPI |
| Дополнительная подробная информация по DPI-PEF:<br>1) Тракт обработки пакетов | |
| 1.1) Функция идентификации пакетов DPI (DPI-PIF)<br>Пример функционального разложения: | Функциональный элемент, отвечающий за обработку условий политики DPI в отношении входящего трафика пакетов |
| 1.1.1) Функция сканирования DPI (DPI-ScF) | Функциональный элемент (как часть DPI-PIF), выполняющий функции первоначального сравнения, которые определяются условиями правил политики DPI |
| 1.1.2) Функция анализатора DPI (DPI-AnF) | Функциональный элемент (как часть DPI-PIF), выполняющий функции последующего сравнения, которые также определяются условиями правил политики DPI (например, в отношении элементов заголовка пакетов или содержимого (в полезной нагрузке пакета)) |
| 1.2) Функция выполнения действий DPI (DPI-AcEF) | Функциональный элемент, предназначенный для выполнения операций над рассматриваемыми пакетами согласно идентифицированным действиям в соответствии с правилами политики DPI |
| 2) Функция базы информации о политике DPI (DPI-PIB; Примечание 1) | Функциональный элемент, представляющий базу данных, которая содержит набор из одной или нескольких записей правил политики DPI (см. ниже) |
| a) Запись правила политики DPI | Запись в таблице, которая содержит правило политики DPI (Примечание 2) |
| i) Условие правила политики DPI (сокращенно – правило политики) | Выражение (как правило, булевого типа). Условие также называется также критерием совпадения (например, для типов состояния, представляющих частичное совпадение, полное совпадение, совпадение префиксов, самое длинное совпадение префиксов и т. д.) |
| ii) Действие в соответствии с правилами политики DPI (сокращенно – действие в соответствии с правилами) | Действие, которое выполняется после оценки всех условий политики в зависимости от правил и заключения о выполнении данного действия |

ПРИМЕЧАНИЕ 1. – Называется также *таблица правил, библиотека сигнатур политики или просто библиотека сигнатур*.

ПРИМЕЧАНИЕ 2. – Может быть применено одно или несколько правил. Подобные правила могут быть статически предопределены (через управление конфигурацией узла передачи пакетов, которое называется управление политикой DPI) или же информация по ним может быть передана (через интерфейс контроля за политикой), а кроме того, они могут на локальном уровне динамически генерироваться (через локальную функцию PDF). Правила политики DPI используются для сравнения информации о контроле за протоколом (PCI, т. е. за элементами заголовка пакета) или о полезной нагрузке/содержимом потоков пакетов с набором условий для определения того, является ли соответствие строк успешным.

### 7.5 Модели отказоустойчивости

Надежность и готовность сетевого узла (например, узла DPI) имеют большое значение для сети, в которой развертывается сетевой узел. Когда сетевой узел в нерабочем состоянии (см., например, модель рабочего состояния в [ITU-T X.731]), это может привести к аварийной ситуации в сети, при которой вероятно, что всем пользователям сети будет принудительно присвоен статус "оф-лайн". Это приведет к утрате большого объема ценной информации. Таким образом, необходимо добиваться высокой надежности и готовности сетевого узла. Как разновидность сетевого узла, узел DPI также должен поддерживать высокую надежность и готовность.

Используя метод отказоустойчивости, группа избыточности "1+N" DPI нацелена на повышение надежности и готовности сети, развернутой с узлами DPI.

Надежность группы избыточности "1+N" DPI может быть рассчитана по следующим параметрам:

1 MTBF – среднее время наработки на отказ – это среднее время между отказами группы избыточности "1+N" DPI;

2 MTTR – среднее время ремонта – это время, затраченное на восстановление нормальной работы отказавшей группы избыточности "1+N" DPI.

Готовность группы избыточности "1+N" DPI может быть рассчитана по следующим формулам (см. [ITU-T G.602]):

3 Готовность = Время безотказной работы/(Время простоя + Время безотказной работы); или

4 Готовность = MTBF/(MTBF + MTTR).

5 В рамках группы избыточности "1+N" количество функциональных компонентов избыточности зависит от конкретной реализации и выходит за рамки сферы применения настоящей Рекомендации. Функциональные компоненты в рамках группы избыточности работали в активном/резервном режиме, и только одни функциональные компоненты работают в качестве активных, а другие – в качестве резервных функциональных компонентов. Если активные функциональные компоненты находятся в нерабочем состоянии, то один и только один из резервных функциональных компонентов станет новым активным функциональным компонентом, а бывший активный функциональный компонент станет резервным функциональным компонентом.

6 Интерфейс между активным функциональным компонентом и резервным функциональным компонентом, который используется для переключения между активным и резервным функциональными компонентами, не зависит от DPI и определяется реализацией. Таким образом, он не входит в сферу применения настоящей Рекомендации.

7 Представлено несколько моделей отказоустойчивости; показаны, в частности, модель отказоустойчивости на уровне узлов DPI (п. 7.5.1), модель отказоустойчивости на уровне PEF DPI (п. 7.5.2), модель отказоустойчивости на уровне PIB DPI (п. 7.5.3) и модель отказоустойчивости на уровне ядра DPI (п. 7.5.4).

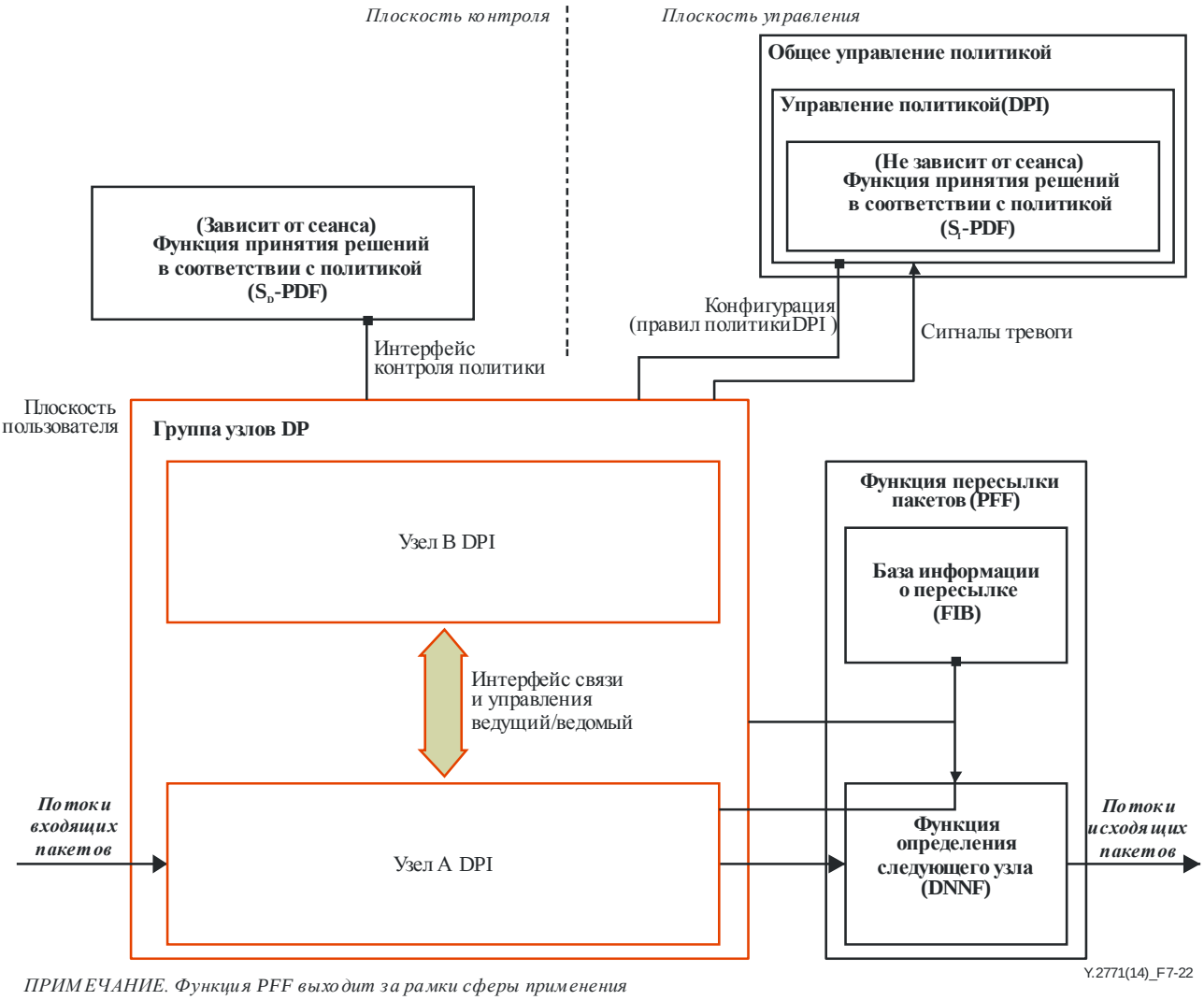
8 Все модели отказоустойчивости основаны на группе избыточности "1+N" DPI (другими словами, избыточности функциональных компонентов, например узлов DPI, см. рисунок 7-22).

9 Активные функциональные компоненты и резервные функциональные компоненты должны сохранять полностью идентичную информацию, такую как PIB, с помощью метода синхронизации данных. Метод синхронизации данных зависит от конкретной реализации и выходит за рамки сферы применения настоящей Рекомендации.

#### 7.5.1 Модель отказоустойчивости на уровне узлов DPI

На рисунке 7-22 изображена модель DPI, гарантирующая надежность на уровне узлов DPI, в которой два или более узлов развертываются совместно для формирования группы узлов DPI (группа избыточности "1+N" DPI, в которой узлы DPI являются функциональными компонентами), а один узел DPI работает в качестве активного узла DPI, тогда как другие работают в качестве резервных узлов DPI. Кроме того, активные и резервные узлы DPI должны дублировать внутреннюю информацию, что необходимо для нормальной работы. Как только активный узел DPI выходит из строя, один из резервных узлов DPI автоматически становится активным узлом DPI.

Несмотря на то что на рисунке 7-22 изображены только два узла DPI, модель отказоустойчивости работает аналогично и в случае, если существует более двух узлов DPI (в соответствии с концепцией избыточности "1+N").




*ПРИМЕЧАНИЕ. Функция PFF выходит за рамки сферы применения настоящей Рекомендации.*

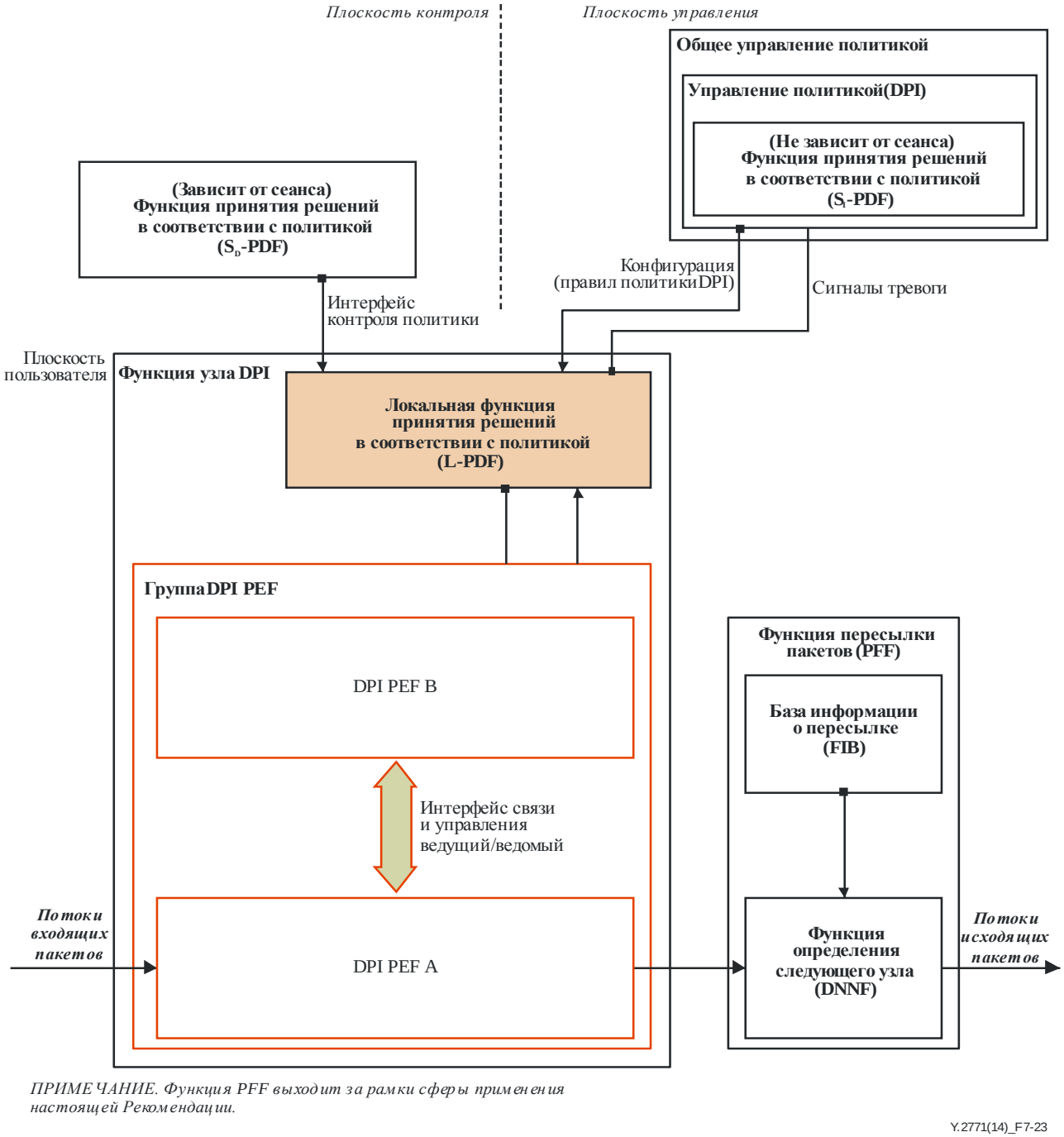
ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.

**Рисунок 7-22. Модель DPI, обеспечивающая надежность на уровне узлов DPI**

### 7.5.2 Модель отказоустойчивости на уровне PEF DPI

На рисунке 7-23 изображена модель DPI с поддержкой надежности на уровне PEF DPI, два или более компонентов PEF DPI (другими словами, группа избыточности "1+N" DPI, функциональными компонентами которой являются компоненты PEF DPI) спроектированы в рамках узла DPI, а один компонент PEF DPI работает в качестве активного компонента, в то время как другие компоненты PEF DPI работают в качестве резервных компонентов. Процедуры переключения в случае отказа аналогичны процедурам при поддержке надежности на уровне узлов (см. п. 7.5.1).

На рисунке 7-23 изображены только два компонента PEF, но несмотря на это модель отказоустойчивости работает аналогично, если существует более двух компонентов PEF.



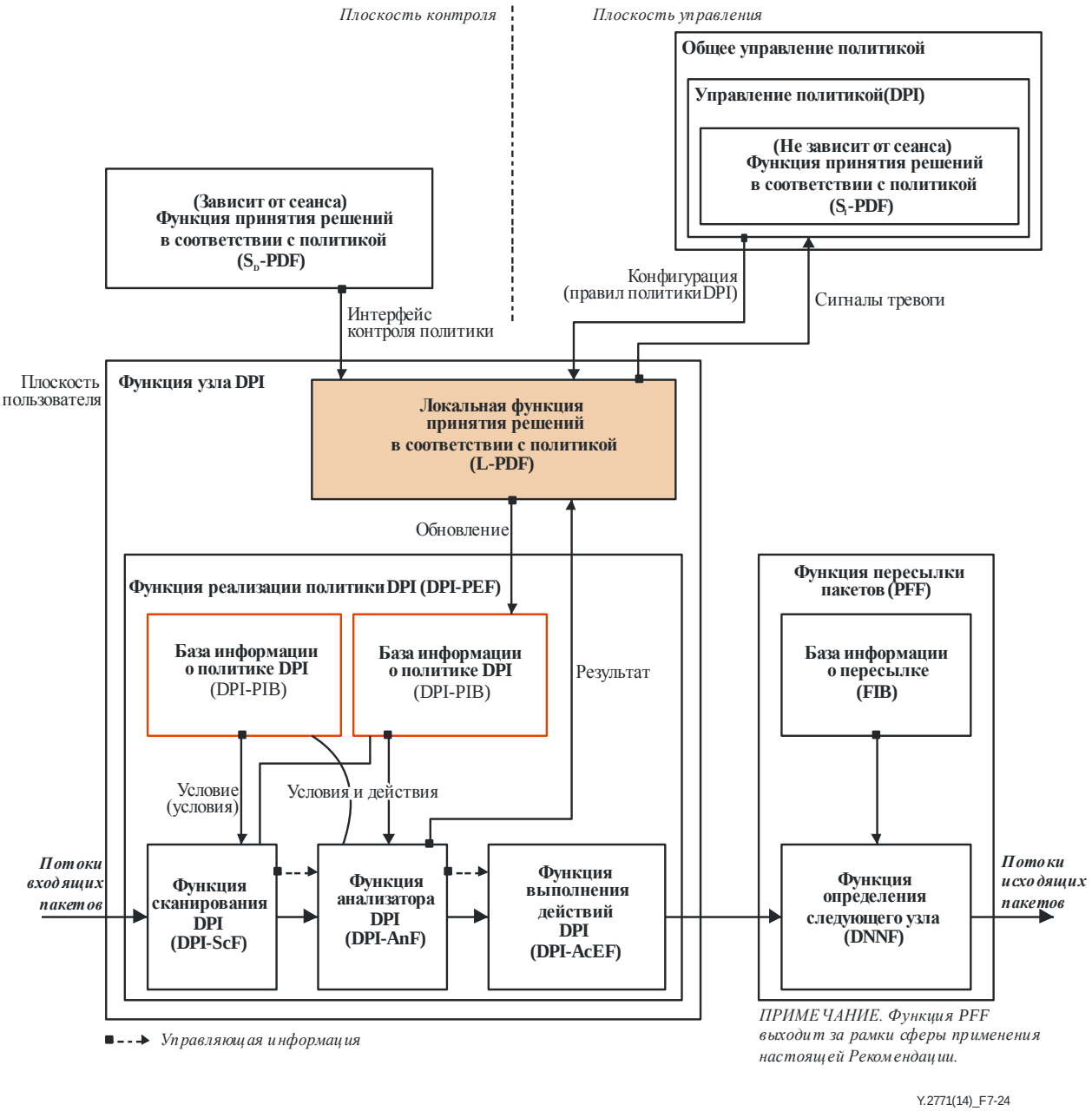

ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.

**Рисунок 7-23. Модель DPI, поддерживающая надежность на уровне PEF DPI**

### 7.5.3 Модель отказоустойчивости на уровне PIB DPI

На рисунке 7-24 отображена модель DPI с поддержкой надежности на уровне PIB DPI, две или более копии PIB DPI (другими словами, две или более копий PIB DPI составляют группу избыточности "1+N" DPI) расположены в узле DPI, а все PIB DPI синхронизированы и, таким образом, содержат одинаковую информацию. Одной из баз PIB DPI присвоена активная роль, а другие базы PIB выполняют резервные функции. Как только активная база DPI выходит из строя, одна из резервных баз DPI автоматически становится активной.

Несмотря на то что на рисунке 7-24 изображены только две базы PIB DPI, модель отказоустойчивости работает аналогично и в случае, если существует более двух баз PIB DPI.



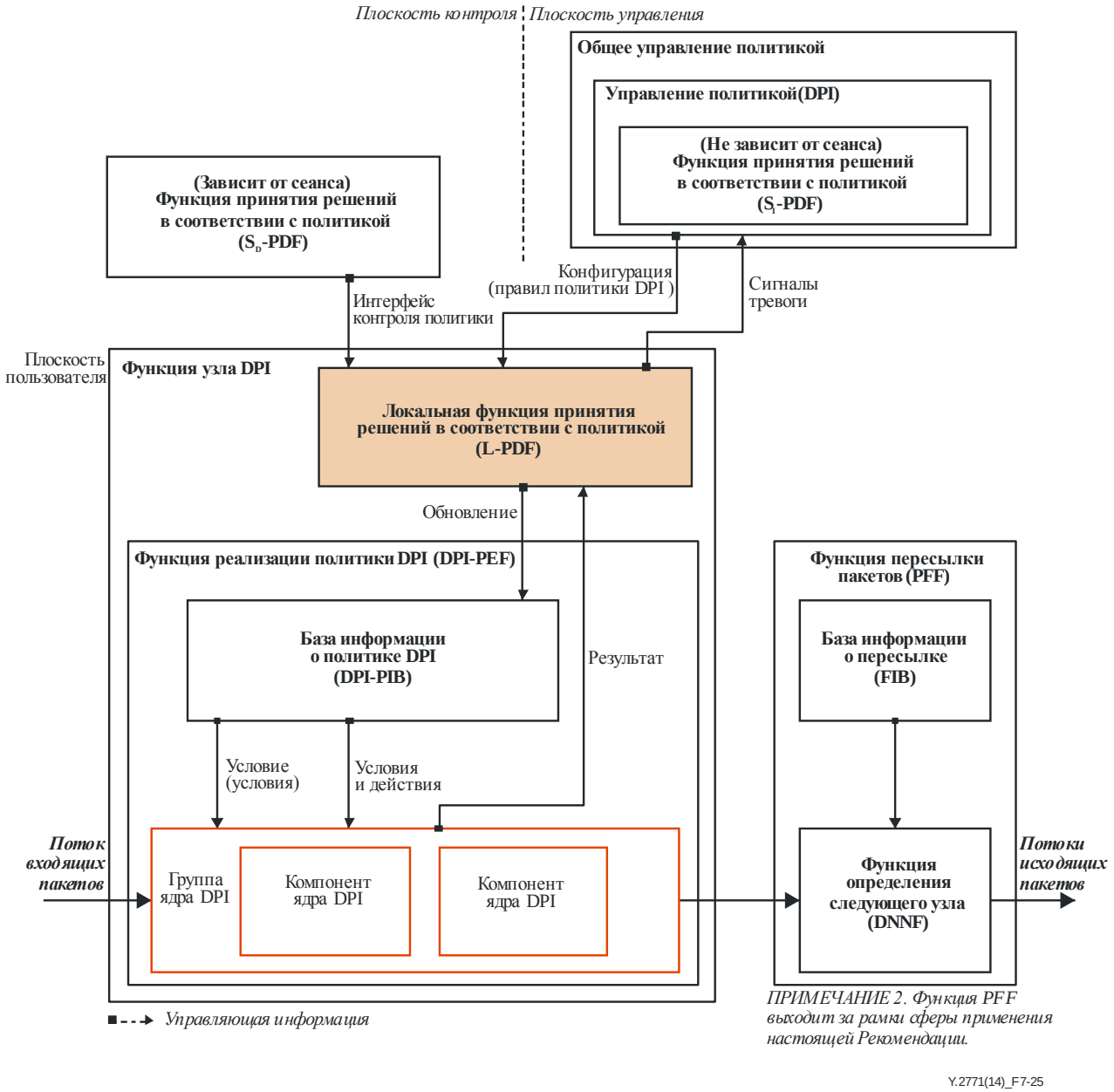

ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.

**Рисунок 7-24. Модель DPI, обеспечивающая надежность на уровне PIB DPI**

### 7.5.4 Модель отказоустойчивости на уровне ядра DPI

На рисунке 7-25 изображена модель DPI, поддерживающая надежность на уровне ядра DPI. Принципы отказоустойчивости аналогичны принципам в предыдущих моделях на более высоких уровнях.

Несмотря на то что на рисунке 7-25 изображены только два ядра DPI, модель отказоустойчивости работает аналогично и в случае, если существует более двух компонентов ядра DPI.




ПРИМЕЧАНИЕ 1. – PFF не входит в сферу применения настоящей Рекомендации.

**Рисунок 7-25. Модель DPI, обеспечивающая надежность на уровне ядра DPI**

# 8 Структура функциональных показателей

## 8.1 Цели и сфера применения соображений, касающихся функциональных показателей

В данном разделе описываются структура и переход к идентификации и разработке метрик функциональных показателей, связанных с DPI. Эти метрики могут использоваться для определения характеристик поведения объектов DPI.

Структура функциональных показателей охватывает в основном следующие области.

1 Метрики функциональных показателей.

Пропускная способность, готовность и показатели работы объекта DPI могут быть охарактеризованы метриками функциональных показателей. Основная цель:

a) уточнение возможности повторного использования существующих метрик функциональных показателей, не относящихся к DPI;

b) подтверждение метрик функциональных показателей для конкретных DPI, которые уже были представлены другими организациями, работающими над вопросами DPI;

c) идентификация новых метрик функциональных показателей для конкретных DPI, которая подразумевает определение подобной метрики; и

d) классификация набора метрик по ключевым показателям работы (KPI) и другим метрикам.

2 Требования к функциональным показателям.

Требования DPI подобного рода связаны с конкретными метриками функциональных показателей. Внедрение зависимых требований к функциональных показателям выходит за рамки сферы применения настоящей Рекомендации. Таким образом, как правило, есть возможность получения качественных или относительных требований к функциональным показателям. Спецификация дополнительных качественных или абсолютных требований к функциональным показателям возможна только для ряда ограниченных областей (например, если максимальный бюджет задержки передачи в узле является предметом рассмотрения в рамках всей сквозной сети...).

3 Контрольные функциональные показатели.

Сравнение показателей является достаточно сложной сферой, в том что касается идентификации и спецификации общепризнанных и значимых сценариев контрольного сопоставления. Определение контрольных показателей DPI, как правило, выходит за рамки сферы применения настоящей Рекомендации. Однако в настоящей Рекомендации может быть представлена информация и руководство по рассматриваемым вопросам с попыткой определить контрольные показатели для объектов DPI.

При определении новых типов метрик функциональных показателей (называемых также показателями работы) необходимо в основном следовать руководящим указаниям, приведенным в [b-IETF RFC 6390]. Такое определение должно включать как минимум:

- название метрики и описание метрики;
- метод измерения или расчета;
- единицу измерения; и, кроме того,
- определение метрики функциональных показателей не должно ограничиваться статистическими параметрами, такими как минимум, максимум, среднее, PDF, отклонение и т. д. Подобные аспекты должны скорее всего рассматриваться в рамках спецификации требований.

## 8.2 Метрики функциональных показателей

### 8.2.1 Обзор – функциональные показатели для узлов DPI

Требования к функциональным показателям связаны с метриками функциональных показателей. Наиболее важные типы метрик называются ключевыми показателями работы (KPI), которые представляют подмножества общего набора метрик.

#### 8.2.1.1 Руководящие указания для классификации метрик функциональных показателей, имеющих отношение к DPI, таких как KPI

В настоящей Рекомендации используется следующее определение KPI (примечание: получено из [ETSI TS 132.410]).

- **Ключевые показатели работы (KPI) в общем случае**

  являются первичными метриками для оценки показателей процесса в виде показателей базовой функции сетевого элемента.

- **Ключевые показатели работы для объектов DPI** ($KPI_{DPI}$)

  $KPI_{DPI}$, согласно сфере применения настоящей Рекомендации, характеризует функциональные показатели ядра DPI (см. п. 3.2.6 [ITU-T Y.2770], называется также трактом обработки пакетов DPI).

ПРИМЕЧАНИЕ. – Понятие "показатель работы" (PI) в настоящей Рекомендации является синонимом метрики функциональных показателей.

Для классификации метрик функциональных показателей DPI по принципу относящихся или не относящихся к KPI следует рассмотреть приведенные ниже критерии. KPI для объектов DPI должны удовлетворять следующим условиям:

1 метрика функциональных показателей должна быть тесно связана с самим трактом обработки пакетов, в котором правила политики DPI применяются к объектам в составе пакетов (и, стало быть, ни к каким иным функциям DPI вне тракта передачи пакетов DPI); и

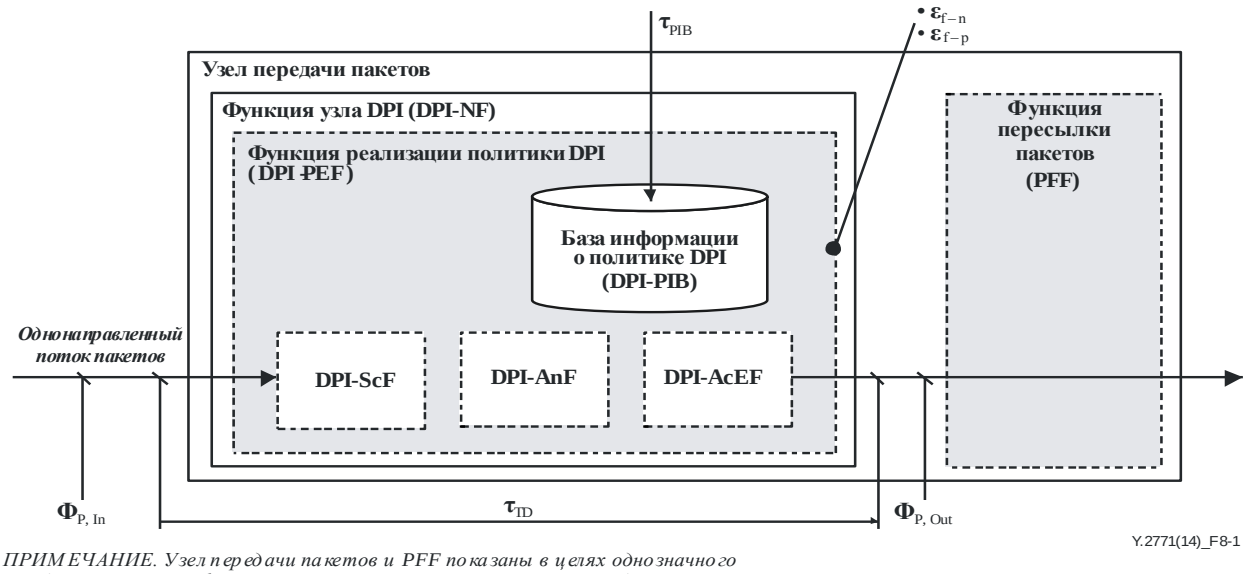
2 метрика функциональных показателей не должна зависеть от сценария использования DPI (следовательно, должна быть независима от приложения для конкретных услуг DPI); и

3 метрика функциональных показателей не должна зависеть от конкретных протоколов ниже и выше уровня IP (следовательно, не должна быть привязана к конкретному транспортному протоколу IP, (такому как TCP), протоколу IP-приложения и т. д.); и

4 метрика функциональных показателей должна быть независима от физических реализаций объектов DPI (следовательно, не должна быть связана с конкретными аспектами реализации, такими как энергопотребление, рассеивание мощности, современные обрабатывающие компоненты и т. д.).

### 8.2.1.2 Типовые ключевые показатели работы для узлов DPI

На рисунке 8-1 показан ряд общеизвестных примеров KPI для узлов DPI (перечень $KPI_{DPI}$ не является исчерпывающим). Перечень видов $KPI_{DPI}$ приведен в нижней части схемы. Соответствующие требования к функциональным показателям (при наличии таковых) изложены в отдельных пунктах.




*ПРИМЕЧАНИЕ. Узел передачи пакетов и PFF показаны в целях однозначного определения метрик функциональных показателей, но сами по себе эти объекты не входят в сферу применения настоящей Рекомендации.*

ПРИМЕЧАНИЕ 1. – Узел передачи пакетов и PFF показаны в целях однозначного определения метрик показателей работы, но оба эти объекта, как таковые, на входят в сферу применения настоящей Рекомендации.
ПРИМЕЧАНИЕ 2. – PFF присутствует только для режима DPI в тракте.

**Рисунок 8-1. Обзор – ключевые показатели работы для узлов DPI**

Важнейшими метриками функциональных показателей являются, как правило, следующие:

- KPI **задержка передачи внутри узла** (DPI) $\tau_{TD}$ [μs]: см. п. 8.2.3.1;
- KPI **скорость обработки пакетов** (DPI) $\varphi_{P,\,In}$ [$s^{-1}$]: см. п. 8.2.3.2;
- KPI **коэффициент ошибок** (DPI) $\varepsilon_{DPI}$: см. п. 8.2.3.3:
  - KPI коэффициент ложноположительных ошибок (DPI) $\varepsilon_{f-p}$;
  - KPI коэффициент ложноотрицательных ошибок (DPI) $\varepsilon_{f-n}$;

- KPI **коэффициент успешно идентифицированных пакетов** (DPI) $\varphi_{P,\ Identified}$ [$s^{-1}$]: см. п. 8.2.3.4.

### 8.2.2 Формальный шаблон для определений метрик функциональных характеристик

Определения метрик функциональных показателей в настоящей Рекомендации используют шаблон, соответствующий таблице 8-1, который в свою очередь получен из шаблона IETF согласно п. 5.4.4 [b-IETF RFC 6390] Performance Metric Definition Template (Шаблон определения метрик функциональных показателей).

**Таблица 8-1. Формальный шаблон для определений метрикфункциональных характеристик**

| | | |
|---|---|---|
| **Название метрики** | N | |
| **Символ** | I | |
| **Описание метрики** | N | |
| **Метод измерения или расчета** | N | |
| **Единицы измерения** | N | |
| **Точка (точки) измерения с потенциальной областью измерений** | N | |
| **Временные характеристики измерений** | N | |
| **Реализация** | I | |
| **Проверка** | I | |
| **Использование и приложения** | I | Например, DPI в реальном времени, DPI не в реальном времени |
| **Модель отчетности** | I | |
| **Тип KPI: да/нет?** | I | Например, KPI, "не KPI" или "не определен" |
| ПРИМЕЧАНИЕ. – Нормативные (N) и информативные (I) элементы описания. | | |

Этот шаблон используется в целях обеспечения определенного минимального качества спецификации для метрик, представленных в настоящей Рекомендации. Однако в связи со "структурным характером" настоящей Рекомендации в ней представлены главным образом *нормативные* элементы описания. Пустые (*информативные*) элементы описания являются признаком того, что для использования подобной метрики в реальной спецификации функциональных показателей в первую очередь необходимо провести дополнительную работу по спецификации в целях получения завершенных, готовых к применению метрик. Например, описание пункта "реализация" выходит за рамки сферы применения "структурной" Рекомендации, вместе с тем определение метрики, не содержащее информации по пункту "проверка", является бесполезным (поскольку требуется, например, для калибровки измерительной функции).

### 8.2.3 Общие определения метрик функциональных показателей для объектов DPI

#### 8.2.3.1 Метрика DPI "внутренняя задержка передачи в узле"

Правила политики, относящиеся к DPI, применяются к каждому отдельному пакету конкретного потока пакетов. Такой вид реализации политики в основном предоставляет дополнительное время обслуживания и ожидания в тракте пересылки пакетов узла передачи пакетов (например, транзитного IP-участка), поддерживающего ядро DPI (т. е. точку реализации политики (PEP), выполняющую функции DPI). Метрика функциональных показателей *внутренняя задержка передачи в узле* представляет задержку передачи пакетов в самом сетевом элементе.

В таблице 8-2 представлено определение этой метрики.

**Таблица 8-2. Метрика DPI "внутренняя задержка передачи в узле"**

| | | |
|---|---|---|
| **Название метрики** | N | Внутренняя задержка передачи в узле |
| **Символ** | I | $\tau_{TD}$ |
| **Описание метрики** | N | Время накопленного ожидания и обслуживания пакета, проходящего через узел DPI |
| **Метод измерения или расчета** | N | Данная величина вычисляется путем измерения значений времени входа и выхода ($T_{in,\,i}$ и $T_{out,\,i}$) отдельных пакетов в интерфейсах передачи пакетов физического или логического представления функции узла DPI.<br>Предварительное условие – объект измерения должен быть способен идентифицировать отдельные пакеты.<br>Предупреждение – данная метрика, как правило, зависит от нагрузки, поскольку внутренняя задержка передачи в узле состоит из значений времени обслуживания и ожидания в узле. Нагрузка, или точнее нагрузка, предлагаемая DPI ADPI-NF, задается скоростью входящего пакета $\varphi_{P,\,In}$ и средним временем обслуживания пакета $T_{H,\,Packet}$ согласно<br>$A_{DPI-NF} = \phi_{P,\,In} \cdot T_{H,\,Packet}$<br>Основная зависимость от нагрузки (см. также п. 8.3)<br>$\tau_{TD} = f(A_{DPI-NF})$ |
| **Единицы измерения** | N | нс |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Данная метрика может использоваться в широком диапазоне временных интервалов |
| **Реализация** | I | – |
| **Проверка** | I | – |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | KPI |
| ПРИМЕЧАНИЕ. – Нормативные (N) и информативные (I) элементы описания. | | |

#### 8.2.3.1.1 Дополнительное обсуждение

a) Узлы DPI по сравнению с узлами, не относящимися к DPI

Пример IP-узла. Задержка передачи узла DPI может быть существенно больше, чем задержка передачи IP-узла традиционного типа (т. е. транзитного IP-участка или маршрутизатора в соответствии с [IETF RFC 1812]), в связи с наличием дополнительной функции обслуживания, добавленной к основным функциональным возможностям IP-пересылки.

b) Типичные взаимосвязи

Внутренняя задержка передачи в узле $\tau_{TD}$ может также зависеть (при определенной реализации) от следующих параметров:

- количества правил политики DPI $N_{db}$ (например, увеличенное время обслуживания при последовательной обработке нескольких правил политики DPI);
- размера пакета $S_p$ [bit] (например, увеличенное время поиска или сравнения как часть проверки условия политики DPI); размер пакета $S_p$ может быть связан со значением размера кадра L2, заданным в [b-IETF RFC2544]; и
- количества ядер DPI $N_{DPIeng}$ (например, учет внутреннего параллелизма, см. п. 7.3.3).

Таким образом, в данном примере $\tau_{TD}$ – это функция параметров $N_{db}$, $S_p$ и $N_{DPIeng}$, т. е. $\tau_{TD} = f(N_{db}, S_P, N_{DPIeng})$.

Три параметра последовательно влияют на среднее время обслуживания пакета, $T_{H,\ Packet}$ (как показано в таблице 8-3): первые два параметра – это факторы увеличения, а третий параметр приводит к сокращению среднего времени обслуживания.

c) Требование качества к функциональному показателю

- Задержка передачи (включая дополнительное время обслуживания, связанное с обработкой DPI) не должна превышать любые сквозные требования в реальном времени, относящиеся к услуге связи в целом.

ПРИМЕЧАНИЕ 1. – Такая возможность пересылки пакетов в обиходе также называется "обработкой скорости передачи данных по проводам".

ПРИМЕЧАНИЕ 2. – Такой функциональный показатель может ограничивать количество применяемых правил политики для пакета (только по причине ограниченного бюджета времени обслуживания).

#### 8.2.3.2 Метрика DPI "скорость обработки пакетов"

В таблице 8-3 представлено определение метрики.

**Таблица 8-3. Метрика DPI "скорость обработки пакетов"**

| | | |
|---|---|---|
| **Название метрики** | N | Скорость обработки пакетов |
| **Символ** | I | $\varphi_{P,\ In}$ |
| **Описание метрики** | N | Скорость передачи пакетов, обработанных DPI-PEF. Это скорость входящих пакетов, поскольку правила политики DPI выполняются для каждого входящего пакета. Скорость исходящего трафика равна или меньше скорости входящего трафика (в связи с возможными действиями по отмене пакета) $\varphi_{P,\ In} \leq \varphi_{P,\ Out}$ |
| **Метод измерения или расчета** | N | Подсчет всех пакетов, полученных на входящем интерфейсе p1 через определенный период времени. Затем значение вычисляется путем деления полученного числа на этот период времени |
| **Единицы измерения** | N | $s^{-1}$ |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Эта метрика в принципе может использоваться в широком диапазоне временных интервалов. Как правило, шкала времени отображается в секундах |
| **Реализация** | I | – |
| **Проверка** | I | – |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | KPI |
| ПРИМЕЧАНИЕ. – Нормативные (N) и информативные (I) элементы описания. | | |

Скорость обработки пакетов DPI $\varphi_P$ зависит от многих параметров, например, от комбинации:

- количества правил политики DPI или размера DPI PIB, $N_{db}$;
- размера пакета, $S_p$. Размер пакета $S_p$ может быть связан со значениями размера кадра L2, заданных в [b-IETF RFC2544]; и
- других возможных параметров.

Пример. Если ($\varphi_P$, $N_{db}$, $S_p$) = (200, 1000, 64), то скорость обработки равна как минимум 200 пакетов в секунду, если количество правил политики меньше 1000, а размер пакета равен 64.

Качественные характеристики описываются в п. 8.3. Обновление DPI-PIB путем добавления новых, изменяющих существующие или исключающих правил политики DPI не должно влиять на номинальную скорость обработки пакетов DPI, $\varphi_P$ (где $\varphi_P$ равно $\varphi_{P, In}$).

#### 8.2.3.3 Метрика DPI "коэффициент ошибок"

Сумма ложноположительного и ложноотрицательного результата называется коэффициентом ошибок узла DPI. Эти метрики функциональных показателей относятся только к статистическим решениям (при наличии таковых) узла DPI. DPI-PEF обеспечивает детерминистский характер для подавляющего большинства правил политики DPI однако могут существовать правила политики DPI с указанием статистических условий политики или потоки пакетов со статистической информацией о трафике, которые могут привести к неправильным решениям функции DPI-PEF.

В таблице 8-4 приведено определение этой метрики.

**Таблица 8-4. Метрика DPI "коэффициент ошибок"**

| | | |
|---|---|---|
| **Название метрики** | N | Коэффициент ошибок |
| **Символ** | I | $\varepsilon_{DPI}$ |
| **Описание метрики** | N | Сумма ложноположительных (см. п. 8.2.3.3.1) и ложноотрицательных (см. п. 8.2.3.3.2) результатов для узла DPI |
| **Метод измерения или расчета** | N | Прямое измерение невозможно (Примечание 2).<br>Косвенное измерение (вычисление)<br>$\varepsilon_{DPI} = \varepsilon_{f-n} + \varepsilon_{f-p}$ |
| **Единицы измерения** | N | – |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Интервал измерения зависит от временной шкалы с позиции отдельного случая для обслуживаемого пользователя (Примечание 3) |
| **Реализация** | I | – |
| **Проверка** | I | – |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | KPI |
| ПРИМЕЧАНИЕ 1. – Нормативные (N) и информативные (I) элементы описания.<br>ПРИМЕЧАНИЕ 2. – Данная метрика функциональных показателей является так называемой составной метрикой, т. е. она не может быть измерена напрямую, но может быть скомпонована из базовых метрик, которые представляют собой результаты измерений (см. п. 5.3.1/[b-IETF RFC 6390]).<br>ПРИМЕЧАНИЕ 3. – Отдельный случай для обслуживаемого пользователя в общем представляет собой удаленный объект ("пользователь"), заинтересованный в результатах измерения. Примеры: система управления функциональными характеристиками, DPI PD-FE. | | |

#### 8.2.3.3.1 Метрика DPI "коэффициент ложноположительных ошибок"

В таблице 8-5 приведено определение этой метрики.

**Таблица 8-5. Метрика DPI "коэффициент ложноположительных ошибок"**

| | | |
|---|---|---|
| **Название метрики** | N | Коэффициент ложноположительных ошибок |
| **Символ** | I | $\varepsilon_{f-p}$ |
| **Описание метрики** | N | Доля отрицательных случаев, которые ошибочно были отмечены как положительные |
| **Метод измерения или расчета** | N | Измерения этой метрики являются сами по себе сложной задачей, поэтому в настоящей Рекомендации могут быть приведены лишь показания приборов.<br>Как правило, объекту DPI посылается стандартный образец из достаточно большой серии пакетов. Ожидаемый результат (заданный применяемыми правилами политики DPI) сравнивается с измеренными результатами, полученными из процесса DPI.<br>Измерение может быть выполнено одним из способов – с вмешательством или без вмешательства. |
| **Единицы измерения** | N | – |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Интервал измерения зависит от временной шкалы с позиции отдельного случая для обслуживаемого пользователя. |
| **Реализация** | I | – |
| **Проверка** | I | – |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | Да |
| ПРИМЕЧАНИЕ 1. – Нормативные (N) и информативные (I) элементы описания. | | |

Пример 1:

Условие $C_i$ политики DPI подразумевает идентификацию "приложения типа X", а функция идентификации пакета (DPI-PEF) принимает "приложение типа X" за "приложение типа Y", что является ложноположительным результатом.

Пример 2:

Вычисление данной метрики возможно для вероятностной DPI на основе фильтра Блума, (см. Дополнение I) со следующими значениями параметров:

- $m$ – размер фильтра Блума в битах;
- $n$ – количество сигнатур в наборе $S$;
- $k$ – количество хэш-функций, используемых для генерации фильтра Блума.

Коэффициент ложноположительных ошибок $\varepsilon_{f-p}$ задается уравнением

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k .$$

Затем вычисленный и ожидаемый результат могут быть проверены при помощи измерений.

#### 8.2.3.3.2 Метрика DPI "коэффициент ложноотрицательных ошибок"

В таблице 8-6 приведено определение этой метрики.

**Таблица 8-6. Метрика DPI "коэффициент ложноотрицательных ошибок"**

| | | |
|---|---|---|
| **Название метрики** | N | Коэффициент ложноотрицательных ошибок |
| **Символ** | I | $\varepsilon_{f-n}$ |
| **Описание метрики** | N | Доля положительных случаев, которые ошибочно были отмечены как отрицательные |
| **Метод измерения или расчета** | N | См. соответствующую запись в таблице 8-6 |
| **Единицы измерения** | N | – |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Интервал измерения зависит от временной шкалы с позиции отдельного случая для обслуживаемого пользователя |
| **Реализация** | I | – |
| **Проверка** | I | – |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | Да |
| ПРИМЕЧАНИЕ 1. – Нормативные (N) и информативные (I) элементы описания. | | |

Пример:

> Условие $C_i$ политики DPI подразумевает идентификацию "приложения типа X", а функция идентификации пакета DPI (DPI-PIF) не идентифицирует "приложение типа X" как "приложение типа X", что является ложноотрицательным результатом.

#### 8.2.3.3.3 Связь с ошибками выполнения

Ядро DPI как рабочая среда выполнения правил политики DPI обладает рядом характерных для нее ошибок. Однако коэффициент ошибок выполнения и метрика DPI "коэффициент ошибок" представляют собой разные функциональные показатели.

Базовая информация.

Например, внештатное событие при выполнении согласно п. 4.1/[b-IETF RFC 4011] предоставляет информацию о концепции ошибок выполнения:

> […] Исключительная ситуация при выполнении (Run-Time Exception (RTE)) – это критическая ошибка обработки языка или функции. Если во время запуска скрипта происходит ошибка "Исключительная ситуация при выполнении", то выполнение данного скрипта немедленно прекращается. Если при обработке какого-либо элемента условие политики сталкивается с ошибкой "Исключительная ситуация при выполнении", то данный элемент не отвечает необходимому условию и соответствующее действие над этим элементом не производится. […]

### 8.2.3.4 Метрика DPI "коэффициент успешно идентифицированных пакетов"

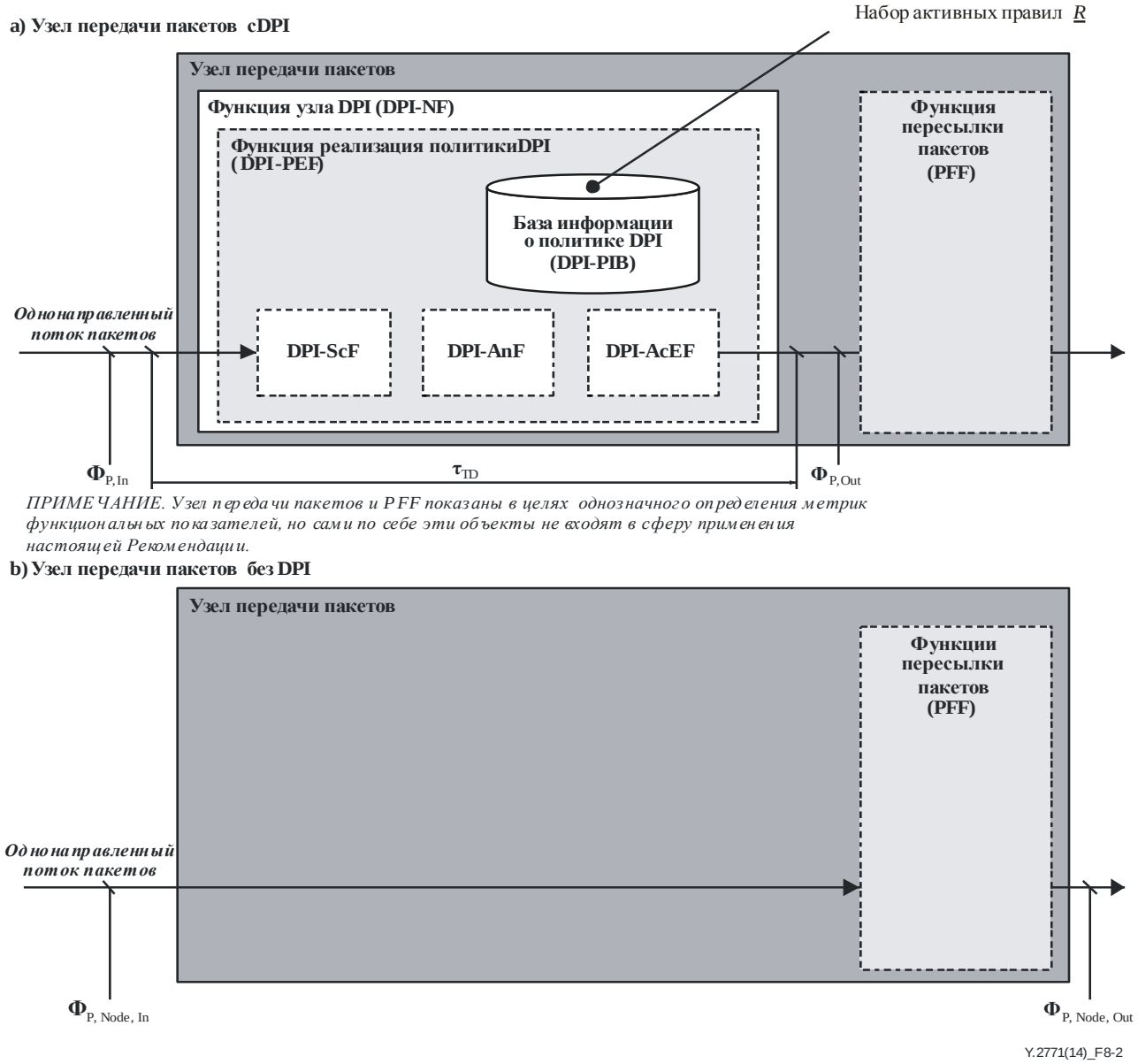
В таблице 8-7 приведено определение этой метрики.

**Таблица 8-7. Метрика DPI "коэффициент успешно идентифицированных пакетов"**

| | | |
|---|---|---|
| **Название метрики** | N | Коэффициент успешно идентифицированных пакетов |
| **Символ** | I | $\varphi_{P,\ Identified}$ |
| **Описание метрики** | N | Входящий пакет успешно идентифицируется (функцией идентификации пакетов), если условия правил политики DPI (как минимум из одного правила политики DPI) "соответствуют" проверяемому пакету.<br>Тип соответствия (полное, частичное, детерминированное, с вероятностью... и т. д.) более подробно не классифицируется.<br>Скорость означает количество успешно идентифицированных пакетов за единицу времени |
| **Метод измерения или расчета** | N | 1 Прямое измерение<br>Например, применение известного правила политики DPI и генерация потока пакетов с известными характеристиками (т. е. соотношение трафика, который должен соответствовать (или не соответствовать), известно заранее). Затем измеренное значение сравнивается с номинальным значением.<br>2 Косвенное измерение (вычисление)<br>$\varphi_{P,\ Identified} = \varphi_{P,\ In} \cdot (1 - \varepsilon_{DPI})$ |
| **Единицы измерения** | N | $s^{-1}$ |
| **Точка (точки) измерения с потенциальной областью измерения** | N | См. рисунок 8-1 (модель трафика) |
| **Временные характеристики измерений** | N | Интервал измерения зависит от временной шкалы с позиции отдельного случая для обслуживаемого пользователя |
| **Реализация** | I | – |
| **Проверка** | I | См. выше метод прямого измерения |
| **Использование и приложения** | I | DPI в реальном времени |
| **Модель отчетности** | I | Обычно как часть управления показателями работы |
| **Тип KPI: да/нет?** | I | KPI |
| ПРИМЕЧАНИЕ 1. – Нормативные (N) и информативные (I) элементы описания. | | |

## 8.3 Функциональные показатели точек реализации политики, оценка показателей характеристик качества

Целью данного раздела является предоставление дополнительной информации относительно количественной оценки функциональных показателей для реализации политики, зависящей от уровня протокола. На рисунке 8-2 показан узел передачи пакетов a) с функцией узла DPI; и b) без применения DPI. В данном случае учитывается такой ключевой показатель, как пропускная способность узла передачи пакетов, $\varphi_{P,\ Node,\ Out}$.




ПРИМЕЧАНИЕ. – Узел передачи пакетов и PFF показаны в целях однозначного определения метрик показателей работы, но оба эти объекта, как таковые, на входят в сферу применения настоящей Рекомендации.

**Рисунок 8-2. Показатели реализации политики – пропускная способность узла передачи пакетов $\varphi_{P, Node, Out}$ в виде функции набора действующих правил политики $\underline{\underline{R}}$ на один пакет**

На рисунке 8-3 показан ряд основных графиков пропускной способности. Специальная функция реализации политики (ось *y*) характеризуется количеством правил политики $\underline{\underline{R}}$ на один пакет, а также аспектами взаимодействия правил. Выполнение конкретного правила политики требует определенного количества ресурсов тракта передачи пакетов в пересчете на процессорное время, память пакетов, память TCAM/CAM, базу данных политики и т. д.

Упрощенное правило гласит: чем больше правил на пакет, тем больше ресурсов требуется для реализации политики.

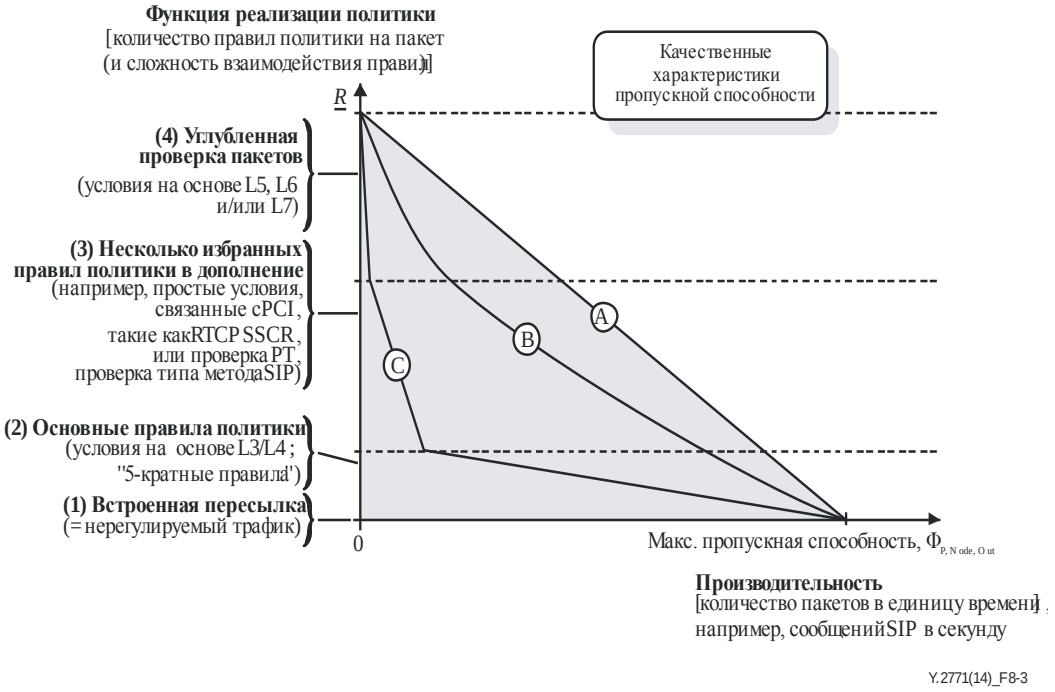



**Рисунок 8-3. Показатели реализации политики – качественные характеристики пропускной способности**

В идеальном случае реализации можно добиться "линейной" характеристики, такой как *A*. Более реалистичная и экономически эффективная модель скорее соответствует кривой *C*.

Технической (и экономической) проблемой, связанной с характеристикой *C*, является достаточно нелинейное отношение, см. рисунок 8-4, в связи с чем проектирование номинальной точки нагрузки и/или достижение необходимого компромисса для ограничения набора выполняемых правил политики становится нетривиальной задачей.

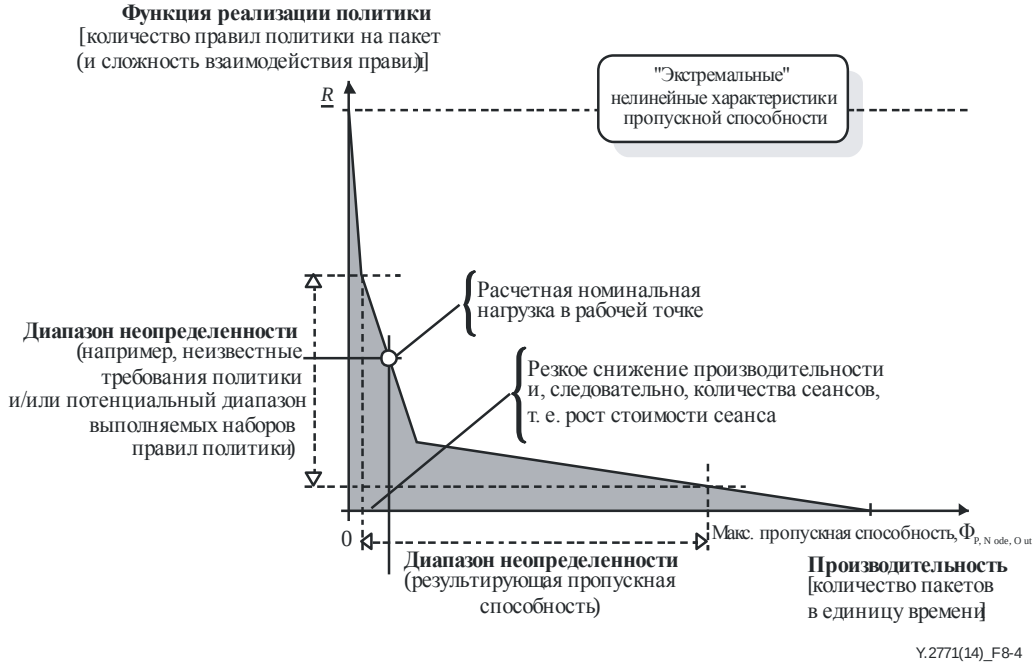



**Рисунок 8.4. Показатели реализации политики – пример использования варианта *C* в качестве наихудшего сценария**

## 9 Классификация функциональных объектов DPI

Объект DPI, как правило, поддерживает не полный набор требований DPI согласно [ITU-T Y.2770], а скорее только подмножество, заданное целевыми вариантами использования. Следовательно, могут существовать различные типы идентифицированных объектов DPI-FE.

### 9.1 Принципы классификации

Каждая подлежащая идентификации функциональная возможность объекта DPI может быть в основном связана с требованиями DPI, как указано в [ITU-T Y.2770]. На высоком уровне существуют:

- функциональные возможности с точки зрения обработки условий;
- функциональные возможности с точки зрения обработки действий; а также, вероятно,
- другие функциональные возможности.

Типичными критериями для идентификации отдельных типов DPI-FE являются сценарии развертывания (вариант использования DPI), сложность обрабатывающей логики, факторы стоимости и т. д.

### 9.2 Функциональные возможности с точки зрения обработки условий

Возможности обработки условий можно разделить на два класса: L4 PI (проверка полезной нагрузки L4 включена) и Non-L4 PI (проверка полезной нагрузки L4 отключена).

### 9.3 Функциональные возможности с точки зрения обработки действий

См. п. 6.3.3.1 в [ITU-T Y.2770], касающийся уровней иерархии действий и примеров.

### 9.4 Типы DPI-FE

В таблице 9-1 использованы принципы классификации из пп. 9.2 и 9.3 и представлен обзор по трем соответствующим типам.

**Таблица 9-1. Категории типов DPI-FE**

<table>
<tr><td colspan="3" rowspan="3">Тип DPI-FE</td><td colspan="2">Функциональные возможности с точки зрения обработки действий</td></tr>
<tr><td colspan="2">Поддержка DPI-AcEF</td></tr>
<tr><td>Нет</td><td>Да</td></tr>
<tr><td rowspan="2">Функциональные возможности с точки зрения обработки условий</td><td rowspan="2">Поддержка проверки полезной нагрузки L4</td><td>Нет</td><td colspan="2">Тип 1</td></tr>
<tr><td>Да</td><td>Тип 2</td><td>Тип 3</td></tr>
</table>

В соответствии с функциональными возможностями DPI-FE конкретный элемент DPI-FE может классифицироваться следующим образом (таблица 9-2).

**Таблица 9-2. Подробное описание трех типов**

| Тип | Обработка правил |
|---|---|
| 1 | FE без возможности проверки полезной нагрузки $L_4$ ($L_4PI = L_4+HI \cup L_7PI$), т. е. тип, не относящийся к DPI-FE (например, SPI-FE) |
| 2 | DPI-FE без возможности выполнения действий (DPI-AcFE), но с проверкой полезной нагрузки $L_4$ ($L_4PI = L_4+HI \cup L_7PI$) |
| 3 | DPI-FE с возможностью выполнения действий (DPI-AcFE) плюс проверка полезной нагрузки $L_4$ ($L_4PI = L_4+HI \cup L_7PI$) |

Тип DPI FE может являться результатом таких факторов, как:

1 количество доступных ресурсов – функциональные возможности конкретного физического объекта DPI (DPI-PE) (например, компоненты аппаратного (HW) или программного (SW) обеспечения); или

2 количество размещенных/задействованных ресурсов для обработки DPI – через управление конфигурацией (например, объекты управления политикой (см. п. 7) путем предоставления выделенного набора функциональных возможностей).

Следует отметить, что конкретный тип *n*-го количества DPI-FE может быть сконфигурирован как тип *m* (*n* > *m*) при помощи своего объекта управления (в связи с тем фактом, например, что "набор функциональных возможностей DPI типа 3" является супермножеством по отношению к прочим типам).

Объект DPI-FE должен быть способен сообщать свой тип связанным функциональным объектам (например, RACF).

В соответствии с функциональными возможностями DPI-FE конкретный элемент DPI-FE типа 3 может далее подразделяться следующим образом (таблица 9-3).

**Таблица 9-3. Подварианты типа 3**

| Тип | Обработка правил |
|---|---|
| 3.1 | DPI-FE с возможностью сбора и отправки информации |
| 3.2 | Тип 3.1 плюс возможность контролировать трафик, но без возможности изменения содержимого пакетов |
| 3.3 | Тип 3.2 плюс возможность изменения содержимого пакетов |

## 10 Вопросы безопасности

Аспекты регулирования, конфиденциальности, приложений безопасности не входят в сферу применения настоящей Рекомендации. При реализации настоящей Рекомендации поставщики оборудования, операторы сетей и поставщики услуг должны учитывать национальные регуляторные требования и требования политики.

Согласно [ITU-Y.2770] объект DPI-FE и информация, касающаяся операций DPI, должны быть защищены от возможных неблагоприятных воздействий. Механизмы, определенные в [ITU-T Y.2704], относятся к требованиям безопасности, приведенным в [ITU-T Y.2770].

# Дополнение I

## Пример функциональной архитектуры вероятностной DPI на основе фильтра Блума

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

### I.1 Введение

Фильтр Блума описывается в [b-Bloomfilter].

"В фильтрах Блума используется метод случайных величин для проверки принадлежности запросов по набору строк. Если задана строка, то фильтр Блума вычисляет по ней *k* хэш-функций, выдавая хэш-величины в диапазоне от 1 до *m* (см. рисунок I-1). Затем он прописывает *k* битов в вектор длиной *m* битов по адресам, соответствующим *k* хэш-величинам, где *k* меньше или равен *m* (см. также уравнение 7-1). Аналогичная процедура повторяется для всех элементов набора. Данный процесс называется программированием фильтра. Процесс запроса аналогичен программированию, при котором строка, принадлежность которой подлежит проверке, является входом в фильтр. Фильтр Блума генерирует *k* хэш-величин, используя те же хэш-функции, что и для программирования фильтра. В векторе длиной *m* битов производится поиск битов в местах расположения, соответствующих *k* хэш-величинам. Если значение хотя бы одного из этих битов оказывается не установленным, то соответствующая строка объявляется не принадлежащей данному набору. Если оказывается, что значение всех битов установлено, то объявляется, что эта строка принадлежит набору с определенной вероятностью. Причиной этой неопределенности в отношении данной принадлежности является тот факт, что эти *k* битов в *m*-битовом векторе могут быть установлены любым из членов. Таким образом, нахождение установленного бита не обязательно подразумевает, что он был установлен конкретной строкой, которая запрашивается. Однако нахождение неустановленного бита однозначно подразумевает, что данная строка не принадлежит набору, поскольку если бы это было так, то все *k* битов были бы установлены при программировании фильтра Блума с помощью этой строки. Этим объясняется наличие ложноположительных и отсутствие ложноотрицательных результатов в данной схеме".

Например, на рисунке I-1 фильтр Блума BF (B[0..m-1]) генерируется тремя хэш-функциями h1, h2 и h3 на строке x1 и x2, где в DPI на основе фильтра Блума строки x1 и x2 являются сигнатурами DPI. Строки y1 и y2 проверяются тремя хэш-функциями h1, h2 и h3 на строках y1 и y2 относительно фильтра Блума BF (заданного битовым вектором B[0..m-1]), где в DPI на основе фильтра Блума строки y1 и y2 представляют структуры проверяемых данных, заданных, например, полезной нагрузкой входящих пакетов.

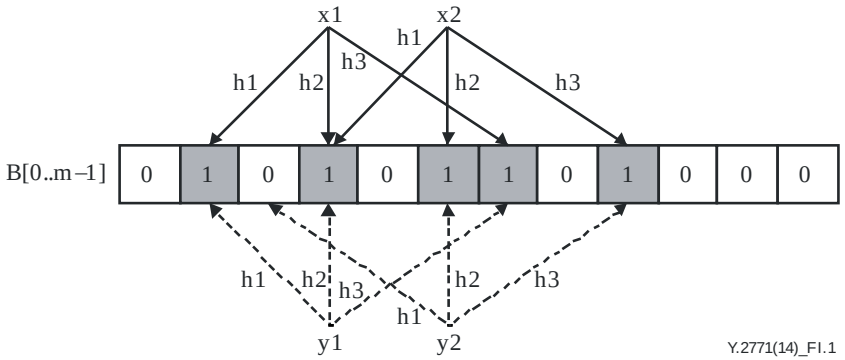



**Рисунок I-1. Программирование и запрос фильтра Блума (BF равен битовому вектору B[0..m-1])**

Коэффициент ложноположительных ошибок $\varepsilon_{f-p}$, выражается уравнением (I-1)

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k, \tag{I-1}$$

где *n* – количество строк, запрограммированных в фильтр Блума. Значение $\varepsilon_{f-p}$ может быть снижено путем выбора подходящих значений *m* и *k* для заданного размера набора элементов *n*.

## I.2 Функциональная модель вероятностной DPI на основе фильтра Блума

Функциональная модель вероятностной DPI на основе фильтра Блума изображена на рисунке I-2. Правило политики для вероятностной DPI может быть следующим.

Если пакет P содержит сигнатуры из набора *S* сигнатур DPI (как условие политики), где набор сигнатур задается значением $S = \{S1, S2..., Sm\}$, то данный пакет отклоняется (как действие в соответствии с политикой).

Фильтр Блума $BF_S$ для набора S сигнатур генерируется набором хэш-функций $H_1$, $H_2$..., $H_k$, Правило политики преобразуется в:

Если $H_1(P)$, $H_2(P)$..., $H_k(P)$ соответствуют $BF_S$, то пакет отклоняется.

Перед тем как анализатор DPI произведет сравнение полученного пакета с данным условием правил политики DPI, сканеру DPI необходимо определить значения сдвига и длины в полученном пакете, которые используются для сопоставления с условиями правил политики DPI.

Существует два основных варианта:

1 Для условий правил DPI при наличии информации о стеке протоколов сдвиг и длина сигнатуры в наборе S известны, сканер передает информацию о сдвиге и длине непосредственно анализатору DPI.

2 Для условий правил DPI, не зависящих от протоколов, сканеру DPI необходимо сканировать и определять сдвиг и длину. Сканер DPI передает эту информацию анализатору DPI.

Анализатор DPI генерирует хэш-величины пакета P с использованием $H_1$, $H_2$..., $H_k$, сопоставляет результаты с $BF_S$, отправляет результаты сопоставления в адрес функции выполнения действий DPI. Функция выполнения действий DPI отправляет результат сопоставления ("истина" или "ложь") и отклоняет пакет, если результат сопоставления оценивается как "истина", в противном случае перенаправляет пакет функции пересылки пакетов. Если сгенерированный результат сопоставления не соответствует $BF_S$, то сканеру DPI необходимо провести сканирование, начиная с байта "offset+1" (offset = offset + 1), и процесс будет продолжен до конца пакета.

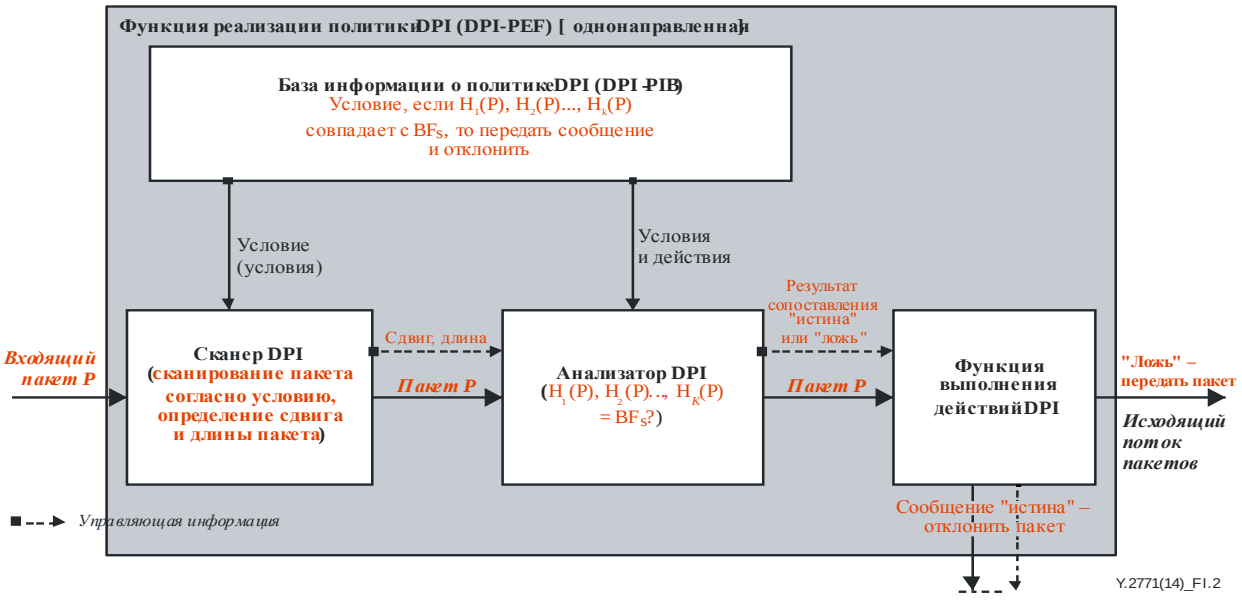



**Рисунок I-2. Функциональная модель вероятностной DPI на основе фильтра Блума**

Следует отметить, что результат сопоставления анализатора DPI является булевой величиной, т. е. "истина" или "ложь", следовательно, он не может представлять собой любое вероятностное значение, например "положительное соответствие с вероятностью *p* (значение *p* находится между 0 и 100%)". Однако весь тракт обработки пакетов DPI поэтапно сам по себе приводит к результатам вероятностной DPI в связи с присущим ему коэффициентом ложноположительных ошибок $\varepsilon_{f-p}$ как части условия политики DPI.

## Библиография


[b-ITU-T H.248.53] Recommendation ITU-T H.248.53 (2009), *Gateway control protocol: Traffic management packages*.

[b-ITU-T I.130] Recommendation ITU-T I.130 (1988), *Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN*.

[b-ITU-T J.380.1] Recommendation ITU-T J.380.1 (2011), *Digital program insertion – Advertising systems interfaces – Advertising systems overview*.

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007), *Framework for creation, storage, distribution and enforcement of policies for network security*.

[b-ITU-T Y.1221] Recommendation ITU-T Y.1221 (2010), *Traffic control and congestion control in IP-based 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-ITU-T Y-Sup.23] ITU-T Y-series Recommendations – Supplement 23 (2013), *ITU-T Y.2770-series - Supplement on DPI terminology*.

[b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[b-IETF RFC 2544] IETF RFC 2544 (1999), *Benchmarking Methodology for Network Interconnect Devices*.

[b-IETF RFC 3060] IETF RFC 3060 (2001), *Policy Core Information Model – Version 1 Specification*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

[b-IETF RFC 4011] IETF RFC 4011 (2005), *Policy Based Management MIB.*

[b-IETF RFC 4292] IETF RFC 4292 (2006), *IP Forwarding Table MIB*.

[b-IETF RFC 6390] IETF RFC 6390 (2011), *Guidelines for Considering New Performance Metric Development*.

[b-Bloomfilter] Dharmapurikar, S. et al., (2003), *Implementation of a Deep Packet Inspection Circuit using Parallel Bloom Filters in Reconfigurable Hardware*. IEEE Proceedings of 11th Symposium on High Performance Interconnects. Stanford University, Wiley, John & Sons, Inc.

[b-CRTC] Canadian Radio-Television and Telecommunications Commission(2009), *ISP Traffic Management Technologies: The State of the Art*.

## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

| | |
|---|---|
| Серия A | 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 |

Отпечатано в Швейцарии
Женева, 2015 г.