Система DPI:
генератор добавленной стоимости седьмого уровня

Юрий СЕНЧЕНКО,
к.т.н., руководитель направления «Широкополосные системы»
ООО «НТЦ ПРОТЕЙ»

Просматривая материалы телекоммуникационных изданий последних лет, нельзя не отметить, что тема интеллектуального управления трафиком пользуется известной популярностью, и популярность эта с каждым годом растет. Выступления представителей телекомов на отраслевых мероприятиях также подтверждают: назначение систем глубокого анализа пакетов (DPI) больше не является вопросом для маркетинговых подразделений операторов связи.

В условиях стабильного роста объемов передаваемых данных участники рынка достаточно синхронно пришли к пониманию, что без инструментов эффективного управления сетью оператор рискует превратиться в низкомаржинальную трубу с неустойчивым качеством обслуживания. Отмеченный запусками сетей LTE в России, 2012 год не стал исключением: операторы связи заранее озвучивают планы по применению систем DPI для выравнивания трафика в случае повышенной загруженности пакетной сети. Опасения операторов по поводу возможной нехватки сетевых ресурсов понятны: новая технология доступа обеспечивает беспрецедентные показатели пропускной способности, открывая путь для терабитных потоков абонентского трафика.

> ***Заблокировав IP-адрес на оборудовании ядра сети, оператор может «легким движением руки» прекратить обмен трафиком с запрещенным сайтом во исполнение требований надзорного органа.***

Основным событием этого года, окончательно зафиксировавшим фокус на теме DPI, тем не менее, стало не внедрение LTE, а вступление в силу 139-ФЗ, вносящего изменения в Закон «О защите детей от информации, причиняющей вред их здоровью и развитию». В соответствии с этим документом интернет-провайдеры обязаны обеспечить техническую возможность ограничения доступа пользователей к материалам, внесенным в «черный» список надзорным органом. В процессе согласования формулировок закона между представителями регулятора, ИТ- и телекоммуникационных компаний были озвучены несколько заслуживающих внимания в контексте настоящей статьи технических моментов.

Как известно, доступ к интернет-ресурсу проще всего ограничить по сетевому (IP) адресу, или, говоря языком ИТ-специалистов, на третьем уровне модели OSI. Заблокировав IP-адрес на оборудовании ядра сети, оператор может «легким движением руки» прекратить обмен трафиком с запрещенным сайтом во исполнение требований надзорного органа. Однако против применения этого подхода ожидаемо высказались компании, предоставляющие услуги хостинга, так как сегодня на одном IP-адресе могут размещаться несколько независимых сайтов, и, блокируя доступ к серверу по третьему уровню, оператор также ограничит доступ абонентов ко всем «соседям» по адресу запрещенного сайта. В попытке соблюсти интересы хостинг-провайдеров и владельцев небольших сайтов, размещающихся на общих IP-адресах, разработчики закона были вынуждены продвигаться «выше» по уровням модели OSI и сформулировали требования по ограничению трафика на седьмом уровне: в реестр помещаются не только IP-адреса, но и доменные имена и (или) указатели страниц с запрещенным содержимым.

Блокирование сайтов по доменным именам является более прецизионным способом ограничения доступа. Оно выполняется путем настройки системы DNS, которая отвечает за преобразование привычных пользователям адресов вида www.example.ru в сетевые адреса для доставки трафика. Этот способ не имеет недостатка блокирования по третьему уровню, так как позволяет отличить «соседей» с одинаковыми IP и произвести блокировку по имени сайта. Однако более-менее опытные пользователи с легкостью распознают основное ограничение данного метода: многие сайты в пределах одного доменного имени разбиты на подразделы, за содержимое которых несут ответственность разные пользователи. Примером сайта такого рода может послужить получивший в последнее время широкую известность Twitter, где на одном и том же доменном имени twitter.com на соседних страницах располагаются блоги звезд шоу-бизнеса, футболистов, ведущих российских политиков и блоги с сомнительным содержимым, потенциально попадающим в категорию запрещенных ресурсов. Блокировка сайта по доменному имени в случае Twitter неприемлема, так как из-за одной компрометирующей огромный портал страницы

пользователи потеряют возможность общаться с любимыми представителями ветвей власти в неформальном режиме 140-символьных сообщений.

Воспользуемся примером Twitter и при рассмотрении способа блокировки по указателю (URL). Оставаясь на том же седьмом уровне OSI, применяющий этот способ интернет-провайдер обойдет ограничения блокировки по доменным именам, так как работа с URL позволяет закрыть доступ к конкретной странице ресурса, не затрагивая законопослушных «соседей». При наибольшей гибкости представленного метода он имеет один недостаток — сложность реализации: если IP-адреса и доменные имена можно блокировать стандартными средствами сетевого оборудования, то для работы с URL потребуется установка системы DPI (*см. рисунок*).

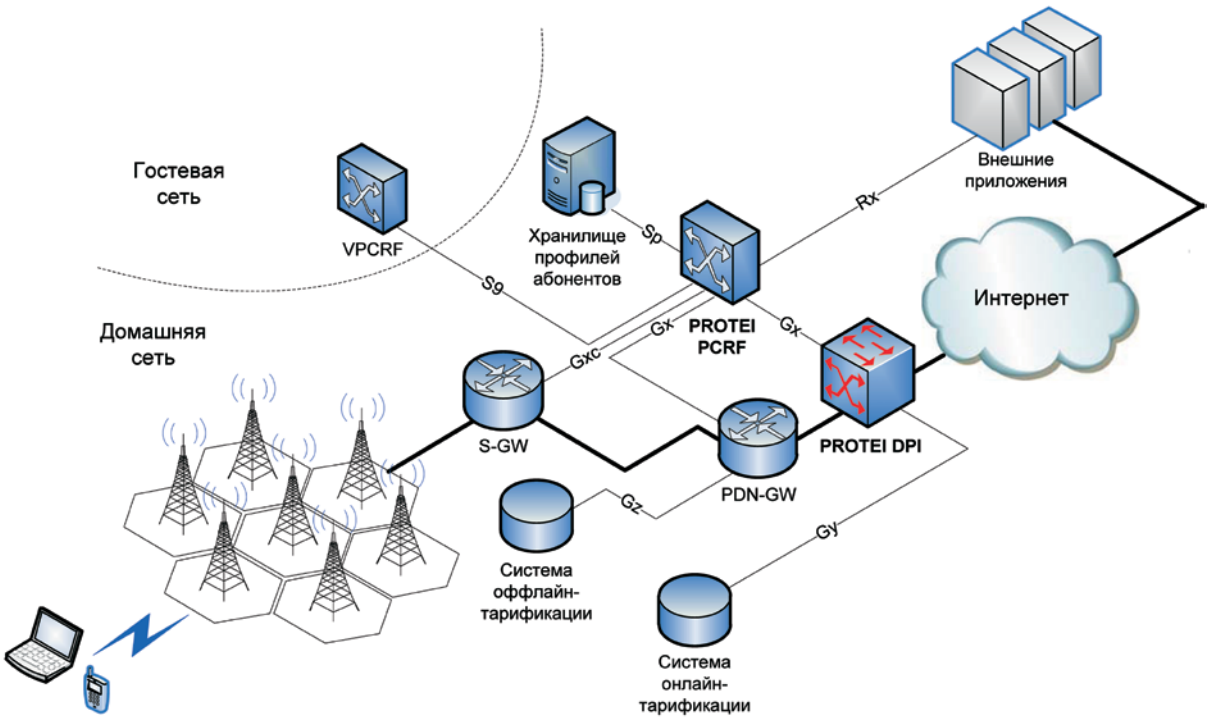
Учитывая стоимость систем анализа трафика, несложно предположить, что интернет-провайдеры не являются большими сторонниками их использования в целях ограничения доступа, так как закупка DPI для приведения сети в соответствие с новым законодательством обернется ростом затрат на инфраструктуру без какого-либо положительного влияния на статью доходов. Однако требования 139-ФЗ не оставляют операторам выбора — блокирование подобных Twitter популярных ресурсов по доменному имени равносильно «ковровой» бомбардировке и повлечет массовый переход абонентов к конкурентам, которые с помощью DPI умеют «точечно» закрывать отдельные страницы без влияния на доступность легитимных разделов сайта.

> ***Разница лишь в том, что в случае закона речь идет о «черном» списке, в то время как «Безопасный Интернет» — это «белый» список ресурсов. Несущественное различие легко регулируется настройками более-менее функциональной системы DPI.***

Таким образом, в очередной раз сложилась ситуация, когда соблюдение общественных интересов требует от операторов некомпенсируемых финансовых вложений. В качестве еще одного свежего примера напрашивается наделавшая много шума кампания по внедрению переносимости мобильных номеров. При неоспоримых преимуществах MNP для потребителей (если колл-центр оператора не отвечает в течение 15 минут, у абонента появляется прекрасная возможность «отомстить») для телекомов затраты на ее реализацию вряд ли могут быть хоть как-то оправданы.

Однако, если сравнивать упомянутые инициативы, ситуация с «черными» списками представляется более благоприятной с точки зрения возврата вложенных средств. С недавнего времени сотовые операторы начали предлагать абонентам услугу «Безопасный Интернет». Услуга популярна среди родителей несовершеннолетних детей — для ограничения контакта с нежелательным содержимым для sim-карты ребенка активируется услуга лимитированного доступа к заранее проверенному списку сайтов, при этом доступ на все прочие сайты закрыт. Предоставление подобной услуги, очевидно, требует наличия системы анализа трафика, аналогичной системе, реализующей функциональность 139-ФЗ. Разница лишь в том, что в случае закона речь идет о «черном» списке, в то время как «Безопасный Интернет» — это «белый» список ресурсов. Несущественное различие легко регулируется настройками более-менее функциональной системы DPI, и оператор, таким образом, получает возможность генерации добавленной стоимости на оборудовании, установленном изначально лишь в целях соблюдения закона.

Возникновение спроса на такую услугу, как «Безопасный Интернет», обусловлено, по всей видимости, двумя



факторами. Первый из них — это техническая возможность, появившаяся с разработкой систем DPI. Вторым фактором является растущая напряженность на просторах Всемирной паутины: процесс вовлечения детей в общение через Интернет посредством социальных сетей, а также увеличение числа устройств с диагональю экрана, достаточной для комфортного просмотра видео, идет параллельно с ничем не ограниченным наводнением Интернета материалами, совершенно непригодными для несовершеннолетних. В подобных условиях желание родителей защитить подрастающее поколение кажется вполне объяснимым.

Действием этих же факторов, вероятно, обусловлено и принятие закона о создании реестра запрещенных ресурсов: в попытке создания безопасного пространства в сети руководство страны регламентирует применение специальных технических средств. При ближайшем рассмотрении требований нового законодательства можно прийти к интересному наблюдению: сравнение механизма действия реестра запрещенных сайтов и механизма реализации

услуги «Безопасный Интернет» дает неожиданный результат. Услуга, предоставляемая операторами связи на коммерческой основе, накладывает на сеть более жесткие ограничения, нежели 139-ФЗ. Закон, действующий по принципу «черного» списка, подразумевает разрешение всего, что не запрещено, в то время как действующая в рамках «белого» списка услуга оператора — запрет всего, что не разрешено. То есть еще до принятия закона абонентами была востребована услуга, предоставляющая заведомо более сильный инструмент защиты от интернет-угроз.

Вероятно, не будет большой ошибкой предположить, что абонентам также интересен более гибкий вариант этой услуги. В качестве примера рассмотрим семью с двумя детьми — дочерью 10 лет и сыном 13 лет. В текущей версии «Безопасного Интернета» родители могут ограничить перечень посещаемых детьми сайтов единым списком проверенных ресурсов, одинаковым для всех пользователей. Представляется, однако, более удобным, если родители смогут отдельно указывать, какие категории сайтов могут быть доступны сыну и дочери. Например, родители наверняка хотели бы закрыть для дочери сайты, посвященные алкоголю, наркотикам, и сайты с откровенным содержимым. Что касается сына, то последнюю категорию некоторые родители могут предпочесть оставить открытой. Другой пример. Наряду с сайтами об алкоголе и наркотиках семья, имеющая антирелигиозные взгляды, скорее всего, пожелает закрыть от детей сайты, посвященные вопросам веры. В то же время семья, регулярно посещающая церковь с детьми, также заблокирует доступ к сайтам с наркотиками, но оставит открытыми для детей ресурсы религиозной направленности (например, сайт воскресной школы). Другими словами, следующим этапом в развитии услуги «Безопасный Интернет» видится персонализированное определение содержимого понятия «безопасность» для каждого абонента в отдельности. Даже самый поверхностный обзор новостных сайтов за последние два-три месяца подтверждает мысль о том, что концепция one size fits all в вопросах религии, политики, воспитания и других «чувствительных» областях, очевидно, несостоятельна.

Дополнительной возможностью уберечь детей от опасности, которую предоставляют современные системы анализа трафика, является уведомление о посещении детьми потенциально опасных ресурсов. Система DPI, распознавая тематическую направленность сайта, может зафиксировать интерес ребенка к нежелательным материалам и отправить соответствующее SMS- или e-mail-сообщение родителям. В условиях доступности в пределах двух кликов информации об изготовлении наркотиков, материалов, призывающих к самоубийству, или пропаганды насильственных действий при отсутствии каких-либо способов ограничения доступа детей к подобным ресурсам вероятность востребованности услуги оповещения родителей представляется достаточно высокой.

В качестве итога представленных рассуждений хотелось бы выдвинуть следующие предположения. Если частью операторов при применении закона о защите детей будет практиковаться «точечное» ограничение доступа к отдельным страницам по URL с помощью систем DPI, остальным операторам так или иначе придется перейти к такому подходу, поскольку блокирование популярных ресурсов на уровне DNS при условии доступности этих же ресурсов у конкурентов станет причиной массового ухода абонентов из сети. Вместе с тем, в настоящее время существует спрос на услуги, основанные на тех же механизмах анализа трафика на седьмом уровне OSI, которые требуются для соблюдения нового законодательства. Таким образом, выбирая оборудование с возможностью фильтрации сайтов и по «черным» (федеральный закон), и по «белым» («Безопасный Интернет») спискам, оператор может предоставлять абонентам генерирующие добавленную стоимость услуги и таким образом преобразовать затраты на приведение сети в соответствие с требованиями закона в инвестиции в развитие новых услуг. Наконец, если устанавливаемая система фильтрации будет в достаточной мере функциональной, оператор сможет на ее основе запустить более гибкие и эффективные услуги по защите детей, обеспечив себе конкурентное преимущество на рынке с давно стагнировавшей абонентской базой. M