УДК 004.716 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1109.html

ОГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ В СЕТИ С ПОМОЩЬЮ ГЛУБОКОЙ ПРОВЕРКИ ПАКЕТОВ ДАННЫХ

В.Д. Смирнов smirnovvd1@student.bmstu.ru
В.Д. Павлова pavlovavd@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Статья посвящена технологии глубокой проверки пакетов (Deep Packet Inspection — DPI), которая представляет собой современный метод анализа сетевого трафика, способный давать информацию о пакетах вплоть до канального уровня передачи данных. В работе рассмотрены основные принципы работы DPI, использование данной технологии для улучшения качества работы сетевых каналов, а также ее применение для мониторинга сетевых угроз и блокирования нежелательного контента внутри сети. Особое внимание уделено преимуществам и рискам, связанным с использованием DPI, а также вопросам эффективности функционирования данной технологии при шифровании пакетов.

Ключевые слова: технология глубокой проверки пакетов, сети, мониторинг трафика, маршрутизация, SSL-инспекция, SSL/TLS

Введение. Технология глубокой проверки пакетов (Deep Packet Inspection — DPI) играет ключевую роль в современной сетевой инфраструктуре, поддерживая высокоэффективные средства для мониторинга и фильтрации информации. В отличие от традиционных методов анализа трафика, основанных лишь на проверке заголовков пакетов, DPI осуществляет проверку содержимого большинства уровней каждого передаваемого пакета, что позволяет более точно настраивать фильтры трафика, выявлять возможные сетевые угрозы и перенаправлять пакеты в случае сбоев на одной из линий связи [1].

Технология DPI возникла в ответ на вызовы, связанные с безопасностью информационных каналов. Ее появление и развитие напрямую зависело от роста объемов передаваемой информации и вычислительных мощностей. В частности, протоколы для передачи голоса (VoIP, voice over internet protocol) и потоковых видео (AVoIP, audio-visual over internet protocol) уже существовали, но средств для их мониторинга не было. Возникла необходимость в более детальном анализе передаваемых данных. Традиционные методы проверки, основанные лишь на сравнении заголов-

 ISSN 2541-8009

ков TCP/UDP[1]-пакетов, стали недостаточными для обнаружения потенциальных угроз.

Наиболее ранние реализации DPI представляли собой специализированное программное обеспечение, которое могло анализировать содержимое пакетов, идентифицировать протоколы и приложения, а также блокировать нежелательный трафик. В этих системах использовались базы данных сигнатур. Однако на тот момент скорость обработки пакетов не была достаточно высокой, что затрудняло использование данной технологии.

Принцип работы DPI. Технология глубокой проверки пакетов основывается на анализе сетевого трафика, что позволяет получать максимально полную информацию о передаваемых данных и осуществлять их контроль и фильтрацию [2]. Основная идея заключается в том, что DPI не ограничивается только анализом заголовков пакетов, как это делают традиционные методы мониторинга, а занимается изучением содержимого каждого пакета (пример стандартной структуры пакета, передаваемого протоколом TCP, показан на рис. 1), что требует высокой вычислительной мощности. В процессе работы DPI устройство или программный модуль получает входящие и исходящие пакеты через сетевой интерфейс, буферизует их и проводит анализ [3].

Рис. 1. Структура TCP/IP-пакета

Первый этап анализа включает проверку заголовков пакетов, в которых фиксируются такие параметры, как IP-адрес отправителя и получателя, номера портов, протоколы, временные метки и служебные поля. Эти проверки позволяют быстро выявить базовую информацию о трафике: его источник,

[1] Здесь и далее под аббревиатурой TCP подразумевается распространенный протокол передачи данных по сети — протокол управления передачей Transmission Control Protocol); под аббревиатурой UDP — протокол пользовательских дейтаграмм User Datagram Protocol.

получателя и тип передаваемых данных. Эту информацию используют для первичной маршрутизации и блокировки недоступных протоколов и адресов.

Однако наиболее важным и сложным является второй этап. На нем проводится глубокий анализ полезной нагрузки, который предполагает изучение содержимого пакета, включая его данные. Основная проблема такой проверки состоит в том, что необходимо расшифровать нагрузку и проверить содержимое, полученное в том числе на прикладном уровне данных. В этом процессе применяются различные методы, а именно:

1) сигнатурный анализ — метод обнаружения угроз и аномалий путем сравнения сетевых данных с заранее определенными шаблонами известных вредоносных файлов или любой другой полезной нагрузки;

2) эвристический подход — метод обнаружения угроз по идентификации заранее определенного набора действий, совершаемого рабочей станцией;

3) методы распознавания семантического содержимого на основе языковых моделей (анализ текстового содержимого полезной нагрузки для поиска запрещенных к распространению данных).

Применяя эти методики, DPI способен точно идентифицировать конкретные приложения или сервисы, распознавая протоколы и форматы данных по их специфическим меткам [4]. После определения характеристик трафика система принимает управляющие решения, основанные на заданных правилах, включая разрешение или блокировку пакетов, ограничение пропускной способности, изменение приоритета обслуживания канала или логирования данных. Пример простой сети с системой контроля и анализа трафика представлен на рис. 2. В этом случае клиент представлен сетевым интерфейсом, его трафик передается на DPI, а результат анализа вместе с пакетом — на сетевой экран (firewall, fw), где после принимается решение о том, сбросить ли пакет (DROP) или разрешить передачу (PASS).

Рис. 2. Структура простой сети с использованием DPI

Такие функции позволяют обеспечивать безопасность сети, предотвращать распространение вирусов, нежелательного контента, а также управлять ресурсами сети для повышения ее эффективности [5]. Кроме того, информа-

 ISSN 2541-8009

ция о заблокированных пакетах сохраняется для последующего аудита. Таким образом, принципы работы DPI основаны на полном и многоступенчатом анализе сетевых пакетов. Благодаря этому она эффективно справляется с обеспечением безопасности и контроля, несмотря на огромные объемы передаваемой информации и сложность современных протоколов и методов шифрования.

Использование DPI для улучшения эффективности сети. Технология глубокого анализа пакетов может быть также применена для увеличения эффективности маршрутизации сетей [6]. Качество и производительность передачи данных в таком случае повышается благодаря выбору оптимальных каналов связи и распределению нагрузки согласно приоритетам. Сеть может быть настроена таким образом, чтобы критически важные приложения получали приоритет при передаче данных. Например, определенным серверам может быть установлен приоритет над всеми остальными клиентами сети. В таком случае пакет данных с этих серверов будут направлены по основным каналам, а оставшийся трафик будет замедлен или отключен. Это позволяет более эффективно использовать пропускную способность сети, разрешая конфликты скоростей при одновременном использовании оборудования.

Дополнительно DPI позволяет организовать динамическую оптимизацию маршрутизации. На основе анализа данных системы могут автоматически перенаправлять трафик, избегая перегруженных сегментов или потенциально нежелательных линий связи. Такой подход обеспечивает более стабильную работу сети и снижает риск возникновения сбоев или замедлений, особенно в условиях высокой нагрузки. Например, правильно настроенный DPI может обнаружить факт компрометации рабочей станции и заблокировать все выходящие и входящие пакеты для нее [7]. Использование DPI также обеспечивает более точное управление ресурсами, поскольку помогает оперативно собирать статистические данные о нагрузке на сеть и считывать ее состояние.

Работа DPI с зашифрованным трафиком. Работа DPI с зашифрованным трафиком представляет собой одну из наиболее сложных и актуальных задач в области современных сетевых технологий, поскольку большинство современных приложений используют вторичное шифрование данных для обеспечения конфиденциальности пользователей. В такой ситуации традиционные методы анализа пакетов становятся практически неэффективными, поскольку содержимое зашифрованных данных недоступно для прямого чтения, что значительно ограничивает возможности DPI при выявлении нежелательного контента [8]. Тем не менее существует несколько подходов и технологий, которые позволяют реализовать работу DPI даже при наличии шифрования.

Одним из методов является анализ метаданных и характеристик трафика. Даже в зашифрованных соединениях многие параметры остаются открытыми для анализа: размеры пакетов, частота их отправки, интервал между ними, направление трафика, использованные протоколы. Эти показатели позволяют делать выводы об источнике отправки и классифицировать его как безопасный или нежелательный. Такой подход широко используется для выявления сетей, в которых применяются специальные средства для обхода блокировок.

Другой метод анализа зашифрованных пакетов — внедрение механизмов, позволяющих применять обычные методики глубокого анализа пакетов при условии соблюдения правил конфиденциальности. В частности, во многих корпоративных сетях используются прокси-сервера или шлюзы, где зашифрованные потоки данных расшифровываются, проходят обработку и логирование и снова шифруются.

В таком случае проводится промежуточная проверка трафика, защищенного протоколом SSL/TLS[2]. Когда пользователь пытается открыть сервис, прокси-сервер получает первичные пакеты и создает зашифрованное SSL/TLS-соединение между собой и клиентом, используя сертификат. Затем он устанавливает соединение с запрошенным сервисом, расположенным на веб-сервере. Прокси-сервер (SSL-прокси) получает возможность расшифровывать передаваемые пакеты и подвергать их глубокому анализу (рис. 3). Таким образом, между приложением и прокси создается соединение по протоколу для защищенного обмена гипертекстом (HTTPS — Hyper Text Transfer Protocol Secure), а между прокси и веб-сервером — соединение для незащищенного обмена гипертекстом (HTTP — Hyper Text Transfer Protocol).

Рис. 3. Схема SSL-инспекции

[2] Secure Sockets Layer — слой защищенных сокетов; Transport Level Security — протокол защиты транспортного уровня.

 ISSN 2541-8009

Таким образом, несмотря на сложности, связанные с работой DPI с зашифрованным трафиком, развитие технологий и стандартов привело к появлению новых решений, которые позволяют работать и с таким видом соединений.

Преимущества и риски при использовании DPI. Технология глубокого анализа пакетов обладает рядом преимуществ и недостатков, которые необходимо учитывать при ее внедрении и использовании.

Среди преимуществ технологии глубокого анализа пакетов можно выделить:

– приоритизацию трафика — DPI позволяет распределять пропускную способность сети более эффективно, давая важным сервисам более высокую пропускную способность;

– мониторинг контента — благодаря технологии глубокого анализа пакетов можно точно настроить, какие данные пользователи сети смогут обмениваться информацией между собой и передавать ее в различные сегменты сети [9];

– обнаружение угроз — эта технология также позволяет выявлять по сигнатурному анализу файлов факты передачи внутри сети вредоносного кода и блокировать их;

– аудит — наконец, благодаря тому, что эта технология обрабатывает каждый пакет на сегменте сети, легко настроить сбор статистики и отчетности для улучшения инфраструктуры и оптимизации использования ресурсов.

Однако у технологии глубокого анализа пакетов также есть ряд серьезных недостатков:

– конфиденциальность — поскольку глубокий анализ пакетов изучает полезную нагрузку, то его работа должна быть регламентирована законодательством [10];

– затраты — DPI требует значительных вычислительных ресурсов для анализа большого объема трафика в реальном времени, что влияет на стоимость внедрения и обслуживания;

– скорость — анализ пакетов в реальном времени требует дополнительной обработки, которая увеличивает задержку, с которой приходит пакет, особенно при интенсивных потоках данных или при использовании сложных методов анализа;

– зашифрованный трафик — при использовании специальных средств для шифрования трафика DPI не сможет распознать вредоносные пакеты и своевременно их заблокировать.

Заключение. Технология глубокого анализа пакетов является мощным инструментом для управления сетевым трафиком. Она позволяет одновременно следить за состоянием инфраструктуры, проводить мониторинг

и фильтрацию передаваемой информации, а также настраивать правила маршрутизации. Однако в то же время ее использование значительно увеличивает нагрузку на вычислительные средства и замедляет скорость доставки пакетов. Таким образом, ее использование для невысоконагруженных сетей нецелесообразно.

Литература

[1] *Краткий обзор технологии DPI — Deep Packet Inspection*. URL: https://habr.com/ru/articles/111054/ (дата обращения 15.10.2025).

[2] Гольдштейн Б.С., Елагин В.С., Зарубин А.А., Фицов В.В. *Методы инспекции пакетов и анализа трафика. Технология Deep Packet Inspection*. Санкт-Петербург, СПбГУТ им. М.А. Бонч-Бруевича, 2018, 60 с.

[3] Кошепаров Д.Я. Программная реализация системы глубокой проверки пакетов. *Вестник науки и образования*, 2020, № 12 (90), ч. 1, с. 21–25.

[4] Воронин В.В. Анализ технологии Deep Packet Inspection. *Вестник Воронежского института высоких технологий*, 2018, № 12 (3). URL: https://www.vestnikvivt.ru/ru/journal/pdf?id=864 (дата обращения 15.10.2025).

[5] Елагин В.С., Онуфриенко В.С. Технология глубокой инспекции пакетов в программно-конфигурируемой сети. *Труды учебных заведений связи*, 2016, № 2, с. 59–63.

[6] Roebuck K. *Deep Packet Inspection (DPI): High-impact Strategies — What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Emereo Publishing, 2011, 183 p.

[7] Романенко О.А. Глубокая инспекция пакетов как средство анализа и контроля трафика. *Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных. Междунар. науч.-техн. семинар: матер*. Минск, Белорусский государственный университет информатики и радиоэлектроники, 2018, с. 90–93.

[8] Фицов В.В. О внедрении DPI. *Вестник связи*, 2016, № 11, с. 25–28.

[9] Гетьман А.И., Евстропов Е.Ф., Маркин Ю.В. *Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений*. URL: https://www.ispras.ru/preprints/docs/prep_28_2015.pdf (дата обращения 15.10.2025).

[10] Mueller M., Kuehn A. Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States. *SSRN Electronic Journal*, 2012. https://doi.org/10.2139/ssrn.2014181

Поступила в редакцию 24.10.2025

 ISSN 2541-8009

Смирнов Вадим Дмитриевич — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Павлова Виталия Дмитриевна — студентка кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Смирнов В.Д., Павлова В.Д., Глинская Е.В. Ограничение доступа к ресурсам в сети через проверку пакетов данных (DPI). *Политехнический молодежный журнал*, 2026, № 03 (104). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1109.html

RESTRICTING ACCESS TO NETWORK RESOURCES WITH DEEP PACKET INSPECTION (DPI)

V.D. Smirnov smirnovvd1@student.bmstu.ru
V.D. Pavlova pavlovavd@student.bmstu.ru
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

This paper examines deep packet inspection (DPI) technology, that is a modern method of network traffic analysis which is capable of working with data link packet levels (within OSI model). The paper describes basic operating principles of DPI, it's usage for improvement of data network service quality and it's abilities to monitor threats within the network and effectively block them. The emphasis is on DPI's general advantages and disadvantages and it's capabilities to work with encrypted traffic.

Keywords: deep packet inspection (DPI), network, traffic monitoring, packet routing, SSL-inspection, SSL/TLS

Received 24.10.2025

Smirnov V.D. — Student of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Pavlova V.D. — Student of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer at the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. of Phys. and Math. Sci., Head of Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Smirnov V.D., Pavlova V.D., Glinskaya E.V. Restricting access to network resources through data packet inspection (DPI). *Politekhnicheskiy molodezhnyy zhurnal*, 2026, no. 03 (104). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1109.html

