

УДК 004.715

URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1116.html>

## СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ВЕБ-ФИЛЬТРАЦИИ КОНТЕНТА

**Е.В. Глинская**

glinskaya@bmstu.ru

SPIN-код: 5430-3023

**В.Д. Смирнов**

smirnovvd1@student.bmstu.ru

**Е.А. Деменева**

demenevaea@student.bmstu.ru

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

Статья посвящена современным технологиям, применяемым для решения задачи веб-фильтрации контента, а именно обеспечения безопасного доступа для авторизованных пользователей, отключения доступа к нежелательному контенту и предотвращения потенциальных информационных атак. Проанализированы методы фильтрации DNS (система доменных имен), в том числе подходы черного и белого списков, использование прокси-серверов и облачных решений сторонних вендоров для обеспечения масштабирования и функционирования сетей. Рассмотрено применение методики глубокого анализа пакетов и ее отличие от привычных способов фильтрации. Особое внимание уделено вопросу адаптации фильтров к постоянно меняющимся угрозам.

**Ключевые слова:** веб-фильтрация, DNS (система доменных имен), глубокая проверка пакетов, VDS (виртуальный частный сервер), маршрутизация

**Введение.** С развитием цифровых технологий задача фильтрации веб-контента не теряет своей актуальности. Каждый год растет количество веб-ресурсов и информационных угроз, от которых компании несут крупные убытки. Веб-фильтрация — это ключевой инструмент, позволяющий ограничивать доступ к таким ресурсам, обеспечивая безопасность пользователей и соблюдение корпоративных стандартов. На данный момент в этой области существуют и развиваются несколько ключевых технологий, таких как DNS-фильтрация (*англ.* Domain Name System — система доменных имен), глубокий анализ пакетов и облачные решения [1].

**DNS-фильтрация.** DNS-фильтрация представляет собой один из основных методов контроля трафика. Каждый пакет, который отправляет клиент в сети, проходит анализ верхних уровней информации, в частности, маршрутизатор изучает принадлежность адреса обращения к списку заблокированных или ограниченных (рис. 1) [2].

Существует несколько вариантов контроля имен — белый и черный списки. Белый список по умолчанию ограничивает все доступные веб-сервисы и оставляет пользователям доступ только к набору адресов, которые были намеренно разблокированы. Такая политика безопасности сильно огра-

ничивает возможности пользователей и может вызывать проблемы доступа для внутренних систем, зависящих от внешних поставщиков [3].



Рис. 1. Схема работы DNS

Черный список работает наоборот. Он запрещает выбранные сайты, оставляя доступ ко всем остальным ресурсам по умолчанию. Такая политика безопасности более мягкая, поскольку не учитывает все возможные угрозы и оставляет пользователям возможность обратиться к потенциально опасным ресурсам.

Как в первом, так и во втором случае необходим список запрещенных или разрешенных ресурсов, актуализация которого служит важным аспектом поддержания уровня работоспособности сети. Чаще всего для обновления этих данных используются системы сигнатурного анализа для проверки на наличие вредоносных файлов, а также реестры угроз. Преимущество такого метода состоит в высокой эффективности для незашифрованного трафика, поскольку отклонение пакетов происходит на этапе разрешения доменного имени.

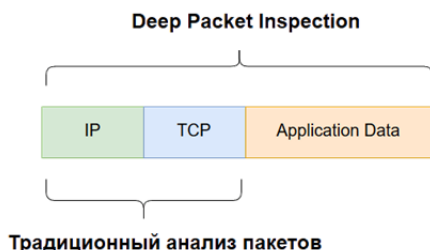


Рис. 2. Сравнение DPI и традиционного анализа пакетов:

IP (Internet Protocol) — интернет-протокол; TCP (Transmission Control Protocol) — протокол управления передачей; Application Data — содержимое пакета

**Глубокий анализ пакетов.** Еще одна технология веб-фильтрации — глубокий анализ пакетов (*англ.* Deep Packet Inspection, DPI). В отличие от рассмотренного выше метода и традиционного анализа пакетов, он позволяет ориентироваться не только на доменные имена, но и на содержание самих веб-ресурсов, а также на их отдельные компоненты (рис. 2). Глубокий

анализ пакетов основывается на проверке всех доступных параметров передаваемого пакета на наличие запрещенных для передачи данных или аномалий трафика [4].

Принцип действия данной технологии состоит в том, что один из серверов сети перехватывает пакеты перед тем, как они ее покидают. Затем он расшифровывает пакеты и анализирует их составляющие [5]: сначала IP-адрес назначения, затем внутреннюю информацию пакета, его состав, размер и дополнительные параметры. Сервер проверяет, есть ли доступ к сети назначения у отправителя, разрешены ли такие протоколы и соответствует ли пакет шаблонам. Содержание пакета проверяется на наличие опасных сигнатур, запрещенной для передачи информации или зашифрованного трафика. Зашифрованный трафик определяется по виду и форме информации, передаваемой по каналу. Например, чаще всего при шифровании трафика используются не типовые размеры пакетов данных, а максимально возможные.

После анализа сервер решает, блокировать ли отправку или разрешить ее, тем самым и проводя веб-фильтрацию данных.

**Облачные решения.** Применение облачных решений часто тесно связано с использованием прокси-серверов в рамках корпоративных сетей [6]. Для веб-фильтрации в таком случае используется подключение к внешнему серверу (клиент подключается по заданному адресу к серверу и пропускает через него трафик своего устройства). Далее сервер ассоциирует клиент с заданным узлом виртуальной сети с определенными настройками (схематический пример подобной сети показан на рис. 3).

Такие решения могут включать в себя перечисленные выше технологии и их комбинацию, а также специальные технические решения, позволяющие выявить аномалии трафика (например, попытку дестабилизировать сервер множественными запросами с разных устройств или попытки множественного несанкционированного доступа с одного устройства) [8].

Таким образом, применение облачных решений позволяет децентрализовать работу систем, разрешив не только физические подключения к серверам, но и распределяя сами сервера, что позволяет более гибко настраивать веб-фильтрацию, например, устанавливая ограничения по различным правилам в разных частях сети [9]. Однако использование облачных решений и организация виртуальной инфраструктуры могут быть связаны с рисками. Так, возможные комбинации правил фильтрации на разных удаленных участках сети могут приводить к конфликтам, результатом которых могут стать сбои проверок на отдельных устройствах или снижение уровня защиты от вредоносных программ. Кроме того, эффективность работы в целом будет зависеть от адаптивности фильтров безопасности [10].

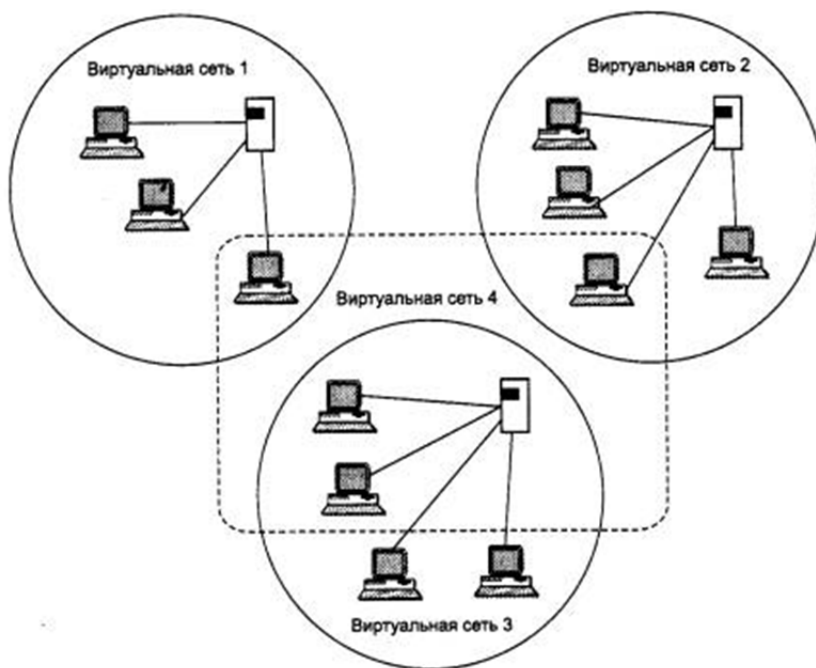


Рис. 3. Пример виртуальной распределенной сети [7]

**Заключение.** Современные технологии веб-фильтрации контента по большей части основываются на анализе содержимого пакетов. Основной проблемой в этой сфере все так же является быстрый рост количества потенциальных угроз и изменение характера их реализации. Вместе с тем использование искусственного интеллекта в рамках исследования вредоносных файлов и информационных пакетов позволило ускорить темпы адаптации к этим угрозам и, как следствие, упростило формирование реестров потенциально опасных веб-ресурсов.

## Литература

- [1] Стрекалов И.Э., Новиков А.А., Лопатин Д.В. Методы динамической фильтрации веб-контента. *Вестник Тамбовского университета. Серия: Естественные и технические науки*, 2014, т. 19, № 2, с. 668–669.
- [2] Kaspersky. Что такое DNS? Принципы работы и уязвимости. Kaspersky Resource Center, 2023. URL: <https://www.kaspersky.ru/resource-center/definitions/dns> (дата обращения 01.12.2025).
- [3] *Реальность в белоснежных списках*. *Habr*, 2025. URL: <https://habr.com/ru/articles/963492/> (дата обращения 01.12.2025).

- [4] Рахметов Р. Deep Packet Inspection (DPI) — что это такое? *Security Vision Blog*, 2025. URL: <https://www.securityvision.ru/blog/deep-packet-inspection-dpi-chto-eto-takoe/> (дата обращения 01.12.2025).
- [5] 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, БГУИР, 2018, с. 90–93. URL: <https://libeldoc.bsuir.by/handle/123456789/36300> (дата обращения 01.12.2025).
- [6] Георгий. Серверные прокси — что это, особенности и примеры использования. *Habr*, 2025. URL: <https://habr.com/ru/articles/957574/> (дата обращения 01.12.2025).
- [7] Газизов Т.Т. *Информационные сети: учебное электронное издание*. Томск, ТГПУ. URL: [https://koi.tspu.ru/koi\\_books/gazizov2/index.htm](https://koi.tspu.ru/koi_books/gazizov2/index.htm) (дата обращения 01.12.2025).
- [8] Cloud4Y. *Облака: в чем преимущество перед корпоративным сервером*. *Habr*, 2019. URL: <https://habr.com/ru/companies/cloud4y/articles/437876/> (дата обращения 01.12.2025).
- [9] Чемодуров А.С., Карпутина А.Ю. Обзор средств фильтрации трафика в корпоративной сети. *Концепт*, 2015, № 2, с. 71–75. URL: <https://e-koncept.ru/2015/15039.htm> (дата обращения 01.12.2025).
- [10] Защита от DDoS-атак в 2025 году: актуальные виды, методы и что реально работает. *Nubes Blog*, 2025. URL: <https://nubes.ru/blog/articles/ddos-2025> (дата обращения 01.12.2025).

**Поступила в редакцию 16.12.2025**

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

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

**Деменева Екатерина Алексеевна** — студентка 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:**

Глинская Е.В., Смирнов В.Д., Деменева Е.А. Современные тенденции веб-фильтрации контента. *Политехнический молодежный журнал*, 2026, № 4(105). URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1116.html>

## MODERN TRENDS IN WEB CONTENT FILTERING

**E.V. Glinskaya**

glinskaya@bmstu.ru

SPIN-code: 5430-3023

**V.D. Smirnov**

smirnovvd1@student.bmstu.ru

**E.A. Demeneva**

demenevaea@student.bmstu.ru

*Bauman Moscow State Technical University, Moscow, Russian Federation*

This paper considers modern web content filtering technologies designed to ensure secure user access to network resources, restrict access to undesirable content, and prevent cyberattacks. The paper analyzes DNS filtering methods, including blacklist- and whitelist-based approaches, as well as the use of proxy servers and third-party cloud solutions to ensure network scalability and operation. Deep packet inspection (DPI) is considered, and its differences from conventional packet filtering methods are discussed. Particular attention is paid to the ability of filtering systems to adapt to constantly evolving threats.

**Keywords:** web-filtering, DNS (Domain Name System), Deep packet inspection, VDS (Virtual Dedicated Server), packet routing

---

***Received 16.12.2025***

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

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

**Demeneva E.A.** — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

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

### **Please cite this article in English as:**

Glinskaya E.V., Smirnov V.D., Demeneva E.A. Modern trends in web content filtering. *Politekhicheskiy molodezhnyy zhurnal*, 2026, no. 4(105). (In Russ.). URL: <https://ptsj.bmstu.ru/catalog/icec/insec/1116.html>