ОГРАНИЧЕНИЯ ТЕХНОЛОГИЙ ГЛУБОКОГО АНАЛИЗА ПАКЕТОВ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ПРОТОКОЛА QUIC: ТЕХНИЧЕСКИЙ АНАЛИЗ И ПОДХОДЫ К АДАПТАЦИИ СИСТЕМ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Рукавицин Эдуард Вячеславович, Карпекин Владимир Александрович

Алтайский государственный технический университет имени И.И. Ползунова, Барнаул
e-mail: ed.rukavitsin@yandex.ru; karpekin05@internet.ru

Аннотация. Массовое внедрение протокола QUIC и работающего поверх него HTTP/3 меняет архитектуру сетевого взаимодействия и снижает эффективность традиционных систем глубокого анализа пакетов (DPI), построенных на разборе TCP-сессий. В статье рассматриваются архитектурные особенности QUIC, затрудняющие классические методы контентной фильтрации: объединение транспортного и криптографического рукопожатий, шифрование служебных полей, использование Connection ID. По RFC 9312 содержимое Initial-пакета (включая ClientHello с SNI) защищено ключами, выводимыми из открытых данных, поэтому SNI извлекается любым наблюдателем на пути; скрывает его только Encrypted Client Hello (ECH). Реальные трудности DPI связаны с многопакетной сборкой ClientHello, отсутствием состояния соединения как в TCP и сменой версий протокола. Приводится качественное лабораторное наблюдение о поведении решения класса NGFW при обработке QUIC-трафика (без количественных оценок). Рассматриваются альтернативные подходы: блокирование UDP-порта 443, отпечатки рукопожатия JA3/JA4, поведенческая классификация, а также влияние ECH, DNS over HTTPS/TLS/QUIC и MASQUE. Делается вывод о необходимости перехода к гибридным архитектурам при учёте рисков избыточно жёстких мер.

Ключевые слова: QUIC, HTTP/3, DPI, глубокий анализ пакетов, контентная фильтрация, шифрование трафика, TLS 1.3, сетевая безопасность, Encrypted Client Hello, классификация трафика.

LIMITATIONS OF DEEP PACKET INSPECTION UNDER THE SPREAD OF THE QUIC PROTOCOL: A TECHNICAL ANALYSIS AND ADAPTATION APPROACHES FOR CONTENT FILTERING SYSTEMS

Rukavitsin Eduard Vyacheslavovitch, Karpekin Vladimir Alexandrovitch

Polzunov Altai State Technical University, Barnaul
e-mail: ed.rukavitsin@yandex.ru; karpekin05@internet.ru

Abstract. The large-scale adoption of the QUIC protocol and HTTP/3 is reshaping network communication and reducing the effectiveness of traditional DPI systems built around TCP session parsing. The article examines QUIC architectural features that complicate classic content-filtering techniques. According to RFC 9312, the Initial packet content (including ClientHello with SNI) is protected by keys derived from public data, so SNI remains observable without ECH. Real DPI difficulties stem from multi-packet ClientHello assembly, lack of TCP-like connection state, and protocol version changes. A qualitative laboratory observation of NGFW behaviour with QUIC traffic is reported (no quantitative estimates). Alternative approaches are discussed: UDP/443 blocking, JA3/JA4 fingerprinting, behavioural classification, and the impact of ECH, encrypted DNS and MASQUE. The article concludes that hybrid architecture is needed, while cautioning against overly rigid measures.

Keywords: QUIC, HTTP/3, DPI, deep packet inspection, content filtering, encrypted traffic, TLS 1.3, network security, Encrypted Client Hello, traffic classification.

За последние годы доля зашифрованного трафика в сети Интернет выросла [1]. Параллельно меняется транспортный уровень: наряду со связкой TCP и TLS используется протокол QUIC, стандартизированный IETF в 2021 году [2] и составляющий основу HTTP/3 [3]. По данным Cloudflare Radar, доля запросов по HTTP/3 составляла около 20,5 % в 2024 году и около 21 % в 2025 году; рост замедлился [4].

Технологии глубокого анализа пакетов (DPI) долгое время рассматривались как один из базовых инструментов контроля приложений и защиты периметра [1]. Работали они преимущественно за счёт характерных признаков TCP-сессий и открытых полей TLS-рукопожатия. Переход на QUIC меняет модель взаимодействия транспортного и криптографического уровней. Цель настоящей статьи — рассмотреть, какие именно архитектурные решения QUIC затрудняют работу DPI-систем, уточнить статус поля SNI и обобщить подходы к адаптации средств контентной фильтрации.

Архитектурные особенности QUIC как причина снижения видимости трафика

Ключевое отличие QUIC от связки TCP и TLS в том, что установление транспортного соединения и криптографического контекста происходит фактически за один обмен пакетами [2, 5]. Уже первый пакет клиента несёт материал рукопожатия TLS 1.3 [6]; способ его защиты определён в RFC 9001 [5]. Поэтому DPI-системе больше не приходится иметь дело с отдельной фазой TCP SYN/SYN-ACK/ACK.

По RFC 9312 [7] содержимое Initial-пакета защищено ключами, которые выводятся из открытых данных (Destination Connection ID и константной соли версии, RFC 9001 [5]). Поэтому ClientHello с полем SNI извлекается любым наблюдателем на пути. Скрывает SNI только механизм Encrypted Client Hello (ECH), стандартизированный как RFC 9849 [8]. Реальные трудности для DPI иные: ClientHello может занимать несколько Initial-пакетов и собирается из

CRYPTO-кадров; состояние соединения не отслеживается так, как в TCP; версии протокола меняются. Рост размера ClientHello, в том числе из-за постквантовых key share, может делать многопакетную сборку обычным случаем; по оценке Cloudflare, постквантовое шифрование использует около половины «человеческого» веб-трафика [4].

Большинство служебных полей QUIC-пакета после установления соединения зашифрованы. Для сохранения сессии при смене IP-адреса используется Connection ID. QUIC работает поверх UDP, что выводит значительную часть трафика из-под фильтров, исторически настраивавшихся на TCP-порт 443. Механизм ненадёжных дейтаграмм (RFC 9221 [9]) свидетельствует о расширяемости платформы, но сам по себе не доказывает снижение видимости для DPI.

Качественное наблюдение: поведение NGFW-решения при обработке HTTP/3-трафика

В ходе тестирования модуля контроля приложений в решении класса NGFW [указать производителя, версию ПО и базы сигнатур], развёрнутом в виртуализированной лабораторной среде, было зафиксировано следующее: правила приложений, построенные на сигнатурном анализе DPI, определяли трафик протестированных сервисов [указать сервисы и версию браузера] при HTTP/2 поверх TLS 1.3 по TCP, но переставали срабатывать при принудительном переключении браузера на HTTP/3. Соединения по QUIC на UDP-порту 443 не попадали под действие профилей приложений и обрабатывались по правилам по умолчанию для UDP-трафика.

Наблюдение носит качественный характер: оно не содержит статистики по числу сессий и доле неопознанных соединений и не позволяет судить о поведении решений других производителей и версий. Результат зависит от версии базы сигнатур и от того, включено ли распознавание QUIC в профиле приложений. Количественная оценка (доля опознанных сессий по сервисам и протоколам, число повторов, тексты правил) — предмет дальнейшей работы.

Подходы к адаптации систем контентной фильтрации

Первый вариант — блокировка исходящего UDP-трафика на порт 443. Клиентские приложения откатываются на TCP и TLS 1.3, для которых остаются механизмы анализа, включая разбор SNI (без ECH). Минус: часть сервисов теряет преимущества QUIC по задержке; для мобильных приложений и CDN возможна деградация [10]. Дополнительно следует учитывать HTTPS-записи DNS (RFC 9460 [11]), которые могут влиять на выбор транспорта.

Второй подход — классификация QUIC-потоков по отпечаткам рукопожатия по типу JA3/JA4, адаптированным под длинный заголовок QUIC. У JA4 есть признак транспорта (QUIC), у JA3 такого нет [12, 13]. Отпечаток позволяет с определённой вероятностью отличать приложения, но требует обновления базы и уязвим к изменению на стороне клиента.

Третий подход — поведенческая классификация потоков по статистическим признакам (размер пакетов, интервалы, характер интенсивности). Методы не требуют доступа к открытым полям и

потенциально устойчивы к усилению шифрования, однако требуют обучающих данных, чувствительны к изменению поведения приложений и дают вероятностный, а не однозначный результат.

Ситуацию усложняет ECH [8]: поле SNI оказывается зашифрованным. Совместно с DNS over HTTPS [14], DNS over TLS [15] и DNS over QUIC [16] сокращается набор наблюдаемых признаков. MASQUE (RFC 9298 [17]) туннелирует UDP через HTTP/3 и скрывает назначение. Практическая мера на конечных точках — отключение QUIC политикой браузера (например, QuicAllowed в Chrome); SSL-инспекция QUIC в общем случае невозможна без терминации на посреднике.

Заключение

Переход части интернет-трафика на QUIC и HTTP/3 — следствие развития транспортных протоколов [1, 2, 7]. Для систем контентной фильтрации это означает необходимость перехода от исключительной опоры на сигнатурный DPI к гибридным архитектурам, сочетающим избирательную блокировку UDP-трафика, отпечатки рукопожатия и поведенческий анализ. Важно учитывать обратную сторону: чрезмерно жёсткие меры способны затронуть легитимные сервисы. Дальнейшие исследования целесообразно направить на повышение точности поведенческой классификации QUIC-трафика и выработку взвешенных политик фильтрации.

Библиографический список

1. RFC 8404. Effects of Pervasive Encryption on Operators [Электронный ресурс] / K. Moriarty, A. Morton (eds.). — IETF, 2018. — URL: https://www.rfc-editor.org/rfc/rfc8404 (дата обращения: 07.10.2026).

2. RFC 9000. QUIC: A UDP-Based Multiplexed and Secure Transport [Электронный ресурс] / J. Iyengar, M. Thomson. — IETF, 2021. — URL: https://www.rfc-editor.org/rfc/rfc9000 (дата обращения: 07.10.2026).

3. RFC 9114. HTTP/3 [Электронный ресурс] / M. Bishop (ed.). — IETF, 2022. — URL: https://www.rfc-editor.org/rfc/rfc9114 (дата обращения: 07.10.2026).

4. Cloudflare Radar 2025 Year in Review [Электронный ресурс]. — Cloudflare, 2025. — URL: https://blog.cloudflare.com/radar-2025-year-in-review/ (дата обращения: 07.10.2026).

5. RFC 9001. Using TLS to Secure QUIC [Электронный ресурс] / M. Thomson, S. Turner (eds.). — IETF, 2021. — URL: https://www.rfc-editor.org/rfc/rfc9001 (дата обращения: 07.10.2026).

6. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3 [Электронный ресурс] / E. Rescorla. — IETF, 2018. — URL: https://www.rfc-editor.org/rfc/rfc8446 (дата обращения: 07.10.2026).

7. RFC 9312. Manageability of the QUIC Transport Protocol [Электронный ресурс] / M. Kühlewind, B. Trammell. — IETF, 2022. — URL: https://www.rfc-editor.org/rfc/rfc9312 (дата обращения: 07.10.2026).

8. RFC 9849. TLS Encrypted Client Hello [Электронный ресурс] / E. Rescorla, K. Oku, N. Sullivan, C. A. Wood. — IETF, 2026. — URL: https://www.rfc-editor.org/rfc/rfc9849 (дата обращения: 07.10.2026).

9. RFC 9221. An Unreliable Datagram Extension to QUIC [Электронный ресурс] / T. Pauly, E. Kinnear, D. Schinazi. — IETF, 2022. — URL: https://www.rfc-editor.org/rfc/rfc9221 (дата обращения: 07.10.2026).

10. Langley A., Riddoch A., Wilk A. [и др.]. The QUIC Transport Protocol: Design and Internet-Scale Deployment // Proceedings of the ACM SIGCOMM 2017 Conference. — Los Angeles, CA, USA, 2017. — P. 183–196. DOI: 10.1145/3098822.3098842.

11. RFC 9460. Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records) [Электронный ресурс] / B. Schwartz, M. Bishop, E. Nygren. — IETF, 2023. — URL: https://www.rfc-editor.org/rfc/rfc9460 (дата обращения: 07.10.2026).

12. Althouse J., Atkinson J., Atkins J. JA3 — a method for profiling SSL/TLS clients [Электронный ресурс]. — Salesforce, 2017. — URL: https://github.com/salesforce/ja3 (дата обращения: 07.10.2026).

13. JA4+ network fingerprinting [Электронный ресурс]. — FoxIO, 2023. — URL: https://github.com/FoxIO-LLC/ja4 (дата обращения: 07.10.2026).

14. RFC 8484. DNS Queries over HTTPS (DoH) [Электронный ресурс] / P. Hoffman, P. McManus. — IETF, 2018. — URL: https://www.rfc-editor.org/rfc/rfc8484 (дата обращения: 07.10.2026).

15. RFC 7858. Specification for DNS over Transport Layer Security (TLS) [Электронный ресурс] / Z. Hu, L. Zhu, J. Heidemann [и др.]. — IETF, 2016. — URL: https://www.rfc-editor.org/rfc/rfc7858 (дата обращения: 07.10.2026).

16. RFC 9250. DNS over Dedicated QUIC Connections [Электронный ресурс] / C. Huitema, S. Dickinson, A. Mankin. — IETF, 2022. — URL: https://www.rfc-editor.org/rfc/rfc9250 (дата обращения: 07.10.2026).

17. RFC 9298. Proxying UDP in HTTP [Электронный ресурс] / D. Schinazi. — IETF, 2022. — URL: https://www.rfc-editor.org/rfc/rfc9298 (дата обращения: 07.10.2026).