**Сравнительная таблица: QUIC vs TLS 1.3 vs TLS 1.2**

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметр** | **QUIC** | **TLS 1.3** | **TLS 1.2** |
| **Транспортный протокол** | UDP | TCP | TCP |
| **Уровень OSI** | Транспортный/Сеансовый | Сеансовый/Представительский | Сеансовый/Представительский |
| **Установление соединения** | 1 RTT (начальное), 0 RTT (восстановление) | 1 RTT (начальное), 0 RTT (восстановление) | 2 RTT |
| **Шифрование по умолчанию** | AEAD (AES-GCM, ChaCha20) | AEAD (AES-GCM) | Различные (CBC-режим и др.) |
| **Алгоритмы шифрования** | AES-GCM, ChaCha20 | AES-GCM, ChaCha20 | AES-CBC, RC4 (устарел) |
| **Forward Secrecy** | Да | Да | Зависит от обмена ключами |
| **Сжатие данных** | Нет (обрабатывается на уровне приложений) | Нет (обрабатывается на уровне приложений) | Поддерживается (но есть проблемы безопасности) |
| **Мультиплексирование** | Да | Нет (зависит от HTTP/2) | Нет (зависит от HTTP/2) |
| **Устой**чи**вость к потере пакетов** | Да (встроенный контроль перегрузок) | Зависит от TCP | Зависит от TCP |
| **Миграц**ия **соединения** | Да | Нет | Нет |
| **Порты** | 443 (UDP) | 443 (TCP) | 443 (TCP) |
| **Поддержка в браузерах** | Chrome, Firefox, Edge | Все основные браузеры | Все основные браузеры |
| **Совместимость** | Средняя (может блокироваться брандмауэрами) | Высокая | Высокая |
| **Безопасность** | Высокая (шифрует больше метаданных) | Высокая (убраны небезопасные алгоритмы) | Средняя (известные уязвимости) |