Совет европейских национальных
регистратур верхнего уровня (CENTR)

Аналитическая записка Совета европейских национальных регистратур верхнего уровня о технологии DNS по HTTPS

Брюссель, Бельгия
17 июня 2019 года

Введение

Аналитическая записка подготовлена Секретариатом Совета европейских национальных регистратур верхнего уровня (CENTR) с целью информирования членов сообщества по вопросам технологии DNS по HTTPS (DoH).

Резюме

При обсуждении технологии DoH важно понимать, что протокол и способ его реализации – не одно и то же. DoH представляет собой протокол, в котором рассматриваются некоторые структурные недостатки системы доменных имен (DNS).[1] Внедрение DoH позволяет устранить такие недостатки, но в то же время ведет к кардинальной перестройке функционирования ключевой составляющей интернета. Разработчики браузеров могут расширить сферу своего влияния и контроля, а их решения повлиять на других участников, вовлеченных в обеспечение стабильного и безопасного пользования интернетом, например на интернет-провайдеров. Такие перемены способны затронуть пользователей, ограничивая свободу выбора, а также возможность государственных органов власти и судов блокировать трафик. Это даже может сказаться на соблюдении принципа универсальности интернета. В результате, все эти последствия будут зависеть от решений нескольких компаний, занимающих доминирующие позиции на рынке интернет-браузеров. В данной записке рассматриваются возможные последствия таких решений.

Мы пришли к выводу, что протокол DoH повышает безопасность интернета, однако способ, которым этот протокол будет реализован, и вытекающая отсюда консолидация рынка могут привести к далеко идущим последствиям.

Краткое описание DoH

Доменное имя представляет собой отображение адреса ресурса в формате, удобном для восприятия человеком, а не в машиночитаемой форме. Использование доменных имен позволяет пользователям запоминать адреса сайтов и электронной почты. Однако доменные адреса не воспринимаются компьютерами и другими устройствами, поскольку для взаимодействия друг с другом они используют IP-адреса. Соответственно, при использовании доменного имени пользователем или приложением, оно должно каждый раз преобразовываться в IP-адрес.

[1] В целях данной статьи под всеми отсылками к системе доменных имен DNS подразумевается только та ее часть, которая будет затронута протоколом DoH. Подробное описание работы системы DNS по адресу: https://centr.org/education/the-dns.html

CENTR vzw/asbl
Belliardstraat 20 (6-й этаж)
1040 Брюссель, Бельгия

Тел: +32 2 627 5550
Факс: +32 2 627 5559
secretariat@centr.org

www.centr.org

Рис. 1 Стандартная схема преобразования доменного имени без использования протокола DNS по HTTPS

В стандартной конфигурации операционная система устройства (ноутбука или мобильного устройства) отправляет резолверу* запрос, который можно сформулировать следующим образом: «Какой IP-адрес закреплен за доменным именем www.example.com?». В настоящее время такой резолвер, как правило, предоставляется интернет-провайдером пользователя.

Система доменных имен представляет собой весьма стабильный и эффективный протокол, не лишенный, однако, недостатков, которые не были учтены на момент его разработки. Можно выделить два основных недостатка:

1. Запросы на преобразование доменного имени отправляются в незашифрованном формате, то есть любой, кто может отслеживать трафик (например, провайдер бесплатного WIFI в кофейне) может видеть, к каким доменам обращаются пользователи такой WIFI-сети.

2. В условиях такой прозрачности возникает риск перехвата запросов и отправки пользователю некорректного ответа. В некоторых случаях результатом может быть неправомерное перенаправление на мошеннические сайты.

**Примечание редактора: Резолвер – программа, которая обеспечивает преобразование доменных имён в IP-адреса.*

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Протокол DNS по HTTPs (DoH) был разработан для устранения этих недостатков. Этот технический протокол был принят Инженерным советом интернета (IETF) в октябре 2018 года.[2]

По сути, DoH представляет собой простое и красивое решение, позволяющее устранить обе проблемы на основе существующих технологий. Это достигается путем отправки запроса по встроенному в браузер протоколу HTTPS. Таким образом, для направления запросов используется браузер, а не операционная система устройства. Этому решению свойственны следующие преимущества: 1. Поскольку такой трафик зашифрован («s» в аббревиатуре HTTPS означает «secure» – «безопасный»), посредник, например, интернет-провайдер или провайдер WIFI, не знает, какие домены посещает пользователь. 2. В результате, перехват трафика и неправильная адресация пользователя становятся практически невозможными (так называемые «атаки посредника»).

Таким образом, DoH бесспорно стал шагом вперед, позволив преодолеть два существенных недостатка первоначальной системы.

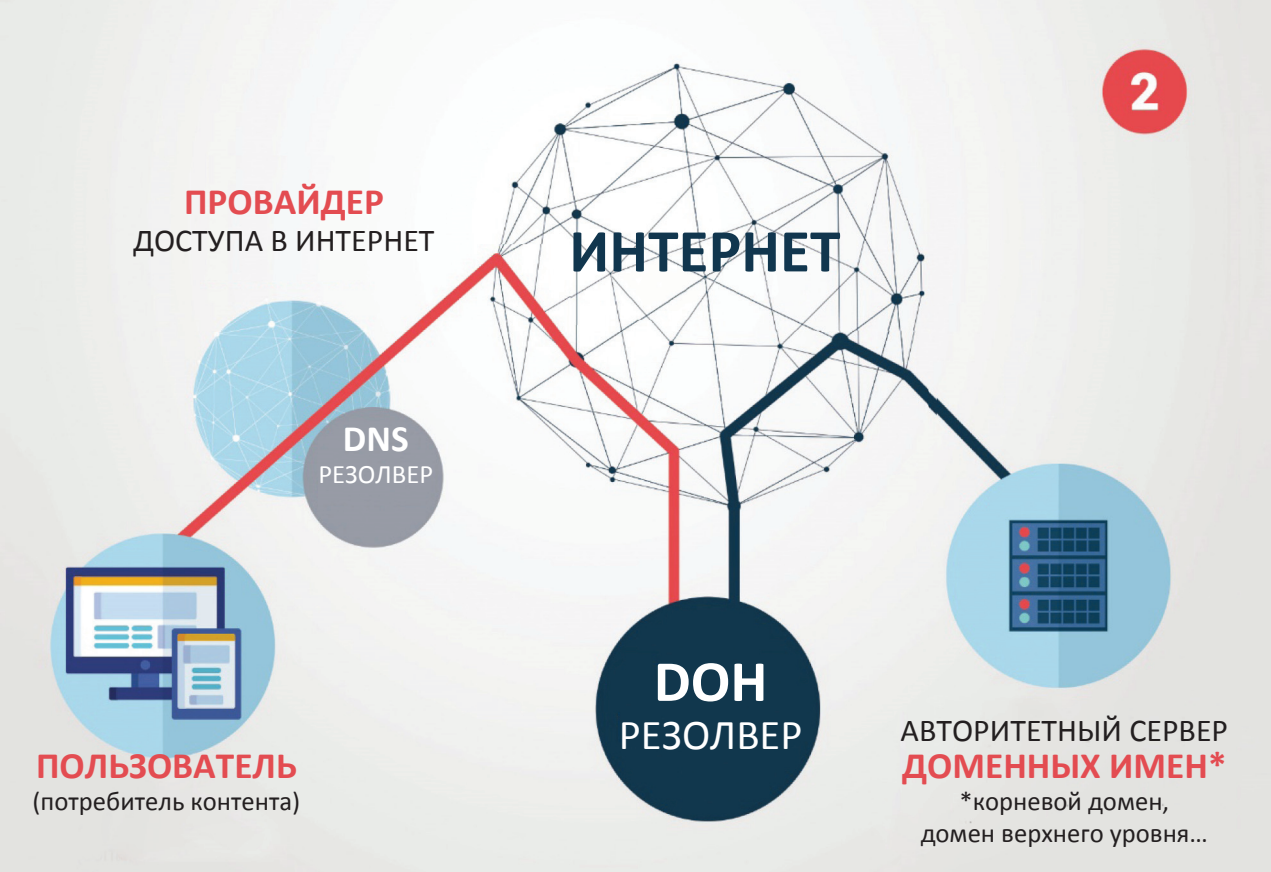

Рис. 2 Схема преобразования доменного имени с использованием протокола DNS по HTTPS

[2] DNS Queries over HTTPS (DoH), RFC 8484. О статусе реализации и самом стандарте можно узнать по адресу: https://datatracker.ietf.org/doc/rfc8484/

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Однако в протоколе не определено, кто должен отвечать на запросы. Это может быть интернет-провайдер, как и раньше, а может быть и другой резолвер. Здесь и начинается самое интересное.

После принятия протокола разработчики браузеров осознали, что могут усилить контроль над трафиком пользователей. Теперь они способны самостоятельно определять, куда (то есть, в какую юрисдикцию) направлять миллиарды запросов каждый день от пользователей по всему миру. Это дает компаниям, занимающимся разработкой браузеров, ощутимые преимущества: они могут лучше контролировать качество навигации, более эффективно обеспечивать безопасность своих пользователей, поскольку упомянутые выше недостатки были устранены, а также выбирать, кто будет преобразовывать запросы.

Все это имело серьезные последствия для интернет-отрасли в целом, связанные не с техническими спецификациями технологии DoH, а с решениями, которые принимают браузеры при ее внедрении.

Последствия применения DoH

Последствия применения технологии DoH подразделяются на три категории: последствия для пользователей, регистратур верхнего уровня и экосистемы интернета.

Последствия для пользователей

Большинство интернет-пользователей находится в счастливом неведении относительно процессов, сопровождающих навигацию в интернете или работу с электронной почтой. Сейчас пользователи могут без труда менять способ преобразования их запросов, однако большинство не знает, зачем это делать и какие варианты у них есть.

Однако возможность свободного выбора имеет большое значение для пользователя. В некоторых случаях это позволяет сделать навигацию в интернете более безопасной, преодолеть некоторые ограничения или цензуру. Это также обеспечивает возможность использования механизмов родительского контроля. Самое главное, что наличие такой возможности позволяет пользователям выбирать резолвер доменного имени, который имеет нужную им политику конфиденциальности. Они могут сделать выбор в пользу резолвера, расположенного в Европе или в США. Важно понимать, что все исходящие от такого пользователя запросы проходят через резолвер, то есть содержат информацию, позволяющую установить личность пользователя и даже его конфиденциальную информацию.

Для пользователей также актуален фактор, который принято обозначать термином «универсальность» интернета. Согласно этому принципу, ответ на запрос должен быть одинаковым вне зависимости от используемого программного обеспечения (поскольку он отправляется операционной системой). В настоящее время выбор конкретного браузера ничего не меняет. Ответ на запрос «Где мне найти www.example.com?» всегда будет одинаковым ввне зависимости "от устройства. Однако с внедрением технологии DoH можно предположить, что различные преобразователи," находящиеся не в одной юрисдикции с пользователем, могут выдавать разные ответы на запросы. В соответствии с требованиями местного законодательства они могут быть обязаны ограничить доступ к контенту, который в юрисдикции пользователя полностью легален. Эта проблема может затронуть лишь ограниченное число доменов, однако выбор браузера способен повлиять на то, в какой навигационной среде окажется пользователь.

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Последствия для регистратур доменов верхнего уровня

С технической точки зрения последствия для регистратур верхнего уровня представляются минимальными. Основным результатом внедрения DoH, скорее всего, станет незначительное снижение потока запросов, направляемых на полномочные DNS-сервера регистратур.

Однако гораздо важнее возможные последствия на политическом уровне. В настоящее время регистратуры верхнего уровня указывают миллионам резолверов по всему миру, каким образом обрабатывать запросы, поступающие из их зоны. Если после успешного внедрения технологии DoH несколько резолверов будут обслуживать 95% интернет-пользователей, это может повлиять на деятельность регистратур верхнего уровня, например вопросы ограничения количества запросов в секунду и соблюдения предписанного срока действительности пересылаемого пакета (Time To Live – TTL).[3]

Последствия для интернет-отрасли

Для понимания возможных последствий внедрения DoH для интернет-отрасли, в первую очередь, необходимо обратить внимание на распределении долей среди участников рынка интернет-браузеров. В настоящее время более 90% рынка контролируется пятью браузерами, что существенно ограничивает выбор потребителей. Требования по совместимости и оптимизации браузеров только усугубляют проблему. Разработчики любого сайта стремятся сократить издержки и оптимизируют его под требования нескольких доминирующих участников рынка (именно поэтому, заходя на сайт, пользователь нередко видит сообщение: «Данный сайт оптимизирован под браузер X»).

Сосредоточение контроля над рынком в руках нескольких браузеров (и определенных ими резолверов) влечет за собой ряд последствий.

Во-первых, хотя на данном этапе это кажется маловероятным, такая ситуация может повлиять на функционирование и развитие системы доменных имен на глобальном уровне. Важно отметить, что соблюдение правил корневой зоны пока осуществляется на добровольной основе. В настоящее время резолвер каждого интернет-провайдера отправляет рекурсивный запрос в корневую зону и действует в соответствии с полученным ответом. Если правила корневой зоны не будут соблюдаться, заказчики быстро перейдут к тем интернет-провайдерам, которые следуют этому правилу. Однако доминирование на рынке ограниченного числа участников снижает вероятность сохранения такой системы. Если по отдельности или сообща они примут решение отказаться от правила корневой зоны, они смогут сделать это без особых проблем. Такие действия будут иметь серьезные последствия для действующей многосторонней модели, в рамках которой под эгидой ICANN ведется разработка политики функционирования корневой зоны. Теоретически, один или несколько резолверов могут решить не принимать запросы для определенного домена верхнего уровня, который, по их мнению, допускает слишком много нарушений, спама и зловредов.

Во-вторых, меняется важная «точка контроля». В настоящее время интернет-провайдер видит трафик DNS и может защитить собственную сеть от злоупотреблений. Самым распространенным примером такой практики является блокировка интернет-провайдерами запросов от зловредного программного обеспечения, установленного на устройствах их клиентов. Блокируя такие запросы,

[3] Считается, что эти требования имеют фундаментальное значение для обеспечения стабильности и безопасности разрешения доменных имен.

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org

интернет-провайдеры повышают безопасность своей сети, а также предотвращают атаки и злоупотребления, связанные с их распространением в других сетях. С переходом на DoH интернет-провайдеры потеряют возможность отслеживать трафик и, соответственно, больше не смогут предотвращать такие злоупотребления.

Существуют и другие последствия. Поскольку интернет-провайдеры имеют возможность контролировать трафик, они могут рассматриваться надзорными органами, судами и правоохранительными органами в качестве стороны, способной оказать содействие в блокировке доступа к нежелательному или незаконному контенту. Например, многие страны Европы ограничили доступ своих граждан к сайту The Pirate Bay. Достичь этой цели они смогли, предписав интернет-провайдерам не пропускать DNS-запросы на доступ к этим доменам, перенаправляя пользователей на сайт, подконтрольный местным правоохранительным органам. Это решение дало возможность быстро (но неэффективно[4]) препятствовать доступу к материалам, размещенным в других юрисдикциях.[5] Однако с технологией DoH блокировка на уровне интернет-провайдера становится невозможной. Уровень контроля будет меняться в зависимости от резолвера, которому браузер направляет запрос. Поскольку такие резолверы в настоящее время расположены в США, они подпадают под юрисдикцию США. Один из таких резолверов (Cloudflare) уже делал заявления о своих намерениях противостоять законодательному и правовому давлению, однако пока неясно, как долго они смогут выдерживать этот натиск.

[4] CENTR, “Analysis of blocking and redirection of domain names as tools to restrict access to content” (Блокировка и перенаправление доменных имен как инструмент ограничения доступа к контенту), см.: https://centr.org/library/library/policy-document/centr-paper-domainblocking-20120302.html

[5]Следует отметить, что в настоящее время даже без технологии DoH пользователи могут выбирать альтернативные открытые рекурсивные DNS-сервера. Это одна из причин неэффективности блокировки. Однако немногие пользователи в настоящее время пользуется этой возможностью..

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Ситуация с внедрением

В начале обзора мы исходили из того, что каждый браузер выбирает один резолвер и указывает его в программном коде. Соответственно, пользователи не смогут поменять его, даже если захотят. Также предполагалось, что эти резолверы будут находиться в США. Все эти предположения основывались на первоначальных заявлениях представителей ряда браузеров и резолверов.

Однако по мере обсуждения этого вопроса стали появляться новые подробности, а разработчики браузеров и резолверы выступили с публичными заявлениями, в которых изложили свои намерения. Так, Mozilla (и выбранный этим браузером резолвер – Cloudflare) заявили, что склоняются к предоставлению ограниченного выбора своим потребителям.[6] Осуществить это можно за счет предоставления пользователям перечня одобренных компанией Mozilla резолверов. Представители Google Chrome (и его собственный резолвер 8.8.8.8) отметили, что позволят интернет-провайдерам сохранить контроль над преобразованием доменных имен, если они смогут предоставить своим пользователям резолвер, совместимый с технологией DoH.[7] Стандарты кодирования обмена информацией между браузером и интернет-провайдером еще только предстоит согласовать.

Дискуссии в рамках Совета европейских национальных регистратур верхнего уровня

В мае 2019 года в Амстердаме состоялась встреча руководителей европейских регистратур верхнего уровня, на которой обсуждалась технология DoH и возможные последствия ее использования. Участники пришли к выводу, что Совету европейских национальных регистратур верхнего уровня следует побуждать своих членов предоставлять открытые рекурсивные DNS-сервера, чтобы дать потребителям более широкий выбор. Некоторые члены Совета европейских национальных регистратур верхнего уровня уже предоставляют такую услугу** (например, регистратуры .lu и .cz).

Дополнительная литература

• V. Bertola, The DoH dilemma: https://www.icann.org/sites/default/files/packages/ids-2019/07-bertola-the-doh-dilemma-dns-symposium-2019-v2-11may19-en.pdf

• G. Huston APNIC DNS over HTTPS Explained: https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/

• O. Guðmundsson, Cloudflare ppt at DNSOARC: https://indico.dns-oarc.net/event/29/contributions/653/attachments/640/1027/DoT_and_DoH_experience.pdf

• О дискуссиях в рамках Инженерного совета интернета см. доклад Совета европейских национальных регистратур верхнего уровня о 104-й встрече Инженерного совета интернета: https://centr.org/library/library/external-event/centr-report-on-ietf104.html

[6] Marshall Erwin, “DNS-over-HTTPS Policy Requirements for Resolvers” (Требования для рекурсивных DNS-серверов к использованию технологии DoH по HTTPS), Mozilla Security Blog, см.: https://blog.mozilla.org/security/2019/04/09/dns-over-https-policy-requirements-for-resolvers/

[7] Согласно заявлению Google Chrome в рамках массовой рассылки Инженерного совета интернета. См.: https://mailarchive.ietf.org/arch/msg/dnsop/dCuB-32Tz5YKCWsrJZ42SXmDs40

***Примечание редактора: В России такую услугу предоставляет MSK-IX – крупнейшая российская точка обмена IP-трафиком.*

LoreCENTR vzw/asbl · Belliardstraat 20 (6-й этаж) · 1040 Брюссель, Бельгия
Тел: +32 2 627 5550 · Факс: +32 2 627 5559 · secretariat@centr.org · www.centr.org