№8
апрель 2018

MSK IX

Интернет изнутри

Глобальная система имен (DNS)

Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №8, дата выхода: апрель 2018 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Чернега Наталья

Корректор:
Рябова Наталья

DNS

главный редактор,
Андрей Робачевский

Дорогой читатель!

Началу практически каждой компьютерной транзакции в Интернете – созданию связи между устройствами для обмена данными – предшествует обращение к глобальной системе доменных имен DNS. DNS настолько фундаментальна для функционирования Интернета, что нарушение ее работы означает нарушение работы Сети в целом.

DNS была стандартизована более 30 лет назад и с тех пор архитектурно претерпела мало изменений. Однако в плане функциональности и использования эволюция DNS весьма значительна: новые записи, связанные с доменным именем, интернационализация DNS, усиление защищенности, в особенности создание расширений DNSSEC. Система доменных имен является ключевым элементом работы сетей доставки контента CDN, важным компонентом решений по безопасности, но также может быть использована как инструмент слежки и сбора персональных данных.

Кстати, в этом выпуске журнала «Интернет изнутри» мы посвятили несколько статей проблемам прослушивания и защиты частной информации, связанным с DNS. Джефф Хьюстон в статье **«Приватность DNS»** наглядно показывает, как DNS может использоваться для «профилирования» пользователей, и рассказывает о направлениях работы по защите и минимизации утечки этих данных. Эту же проблему, но с несколько другой точки зрения, обсуждает **Бенно Оверайндер**. Можно ли добиться сквозной конфиденциальности и защищенности DNS? В чем основная сложность решения этой задачи?

Несмотря на эволюцию DNS, ее часто приводят в качестве примера «окостенения» фундаментальных протоколов Интернета. Система становится жертвой собственного успеха – 30-летнее использование протокола в глобальном масштабе делает значительные изменения непосильной задачей – ведь все пользователи DNS должны «согласиться» с этими изменениями! Однако не все так плохо, замечает **Марк Ноттинхем**, рассказывая, зачем нужно менять Интернет и как это можно сделать. Интересно, что одним из помощников таких изменений является шифрование данных.

Поскольку выпуск посвящен DNS, вы найдете статьи, рассказывающие о многих аспектах этой системы: от защищенности до устойчивости, от новых протоколов до технологий предоставления надежных DNS-услуг. Об одной из таких технологий – технологии **«аникаст»** – расскажет в своей статье известный российский эксперт **Павел Храмцов**.

Как и прошлый номер, мы продолжаем предоставлять журнал в формате EPUB. Надеемся, что планшетники и смартфонники останутся довольны!

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках?
Пишите нам по адресу info@internetinside.ru.

Приватность DNS

Джефф Хьюстон (Geoff Huston)

Да, в наши дни открытость DNS невероятно облегчает его прослушку, перехват и подмену данных; но отчаиваться рано – прилагается много усилий к тому, чтобы создать среду DNS, которая защищала бы конфиденциальность и целостность данных. Минимизация имен запросов позволит значительно сократить уровень утечки информации DNS. А передача запросов и ответов DNS по безопасному каналу затруднит посторонним лицам прослушку и перехват пакетов DNS в пути. Если вдобавок ко всему этому еще и широко распространится DNSSEC, облик Интернета существенно изменится.

Протокол трансляции имен DNS (Domain Name System) пришел к нам еще из тех времен, когда в Интернете царило взаимное доверие, а не нынешняя атмосфера всеобщей подозрительности. DNS – протокол открытый, и свои данные он рассылает направо и налево. Но эти данные – не просто абстрактные непонятные циферки. Запросы и ответы DNS содержат доменные имена для всего, что пользователи делают в Интернете: доменное имя каждого URL, каждой почты, каждого расположения, к которому обращается пользователь. Этот поток данных синхронизирован с действиями пользователей. Практически каждой сетевой транзакции предшествует вызов DNS. Поэтому неудивительно, что в наши дни DNS широко используется для незаявленных целей. Сейчас DNS – не только привычный нам всем протокол трансляции имен, который опрашивает огромную распределенную базу данных, но и потенциальный канал для слежки, а кроме того, способ реализации самых разнообразных способов контроля доступа к контенту в общедоступной сети.

Ситуация с DNS должна измениться. Теперь, когда файлы Сноудена наглядно показали нам, какой масштаб принимают подобные системы слежки – как на службе правительств, так и мотивированные коммерчески, – мы воочию увидели, что многие привычные нам инструменты Интернета слишком доверчивы, слишком болтливы и слишком легко обходятся умным противником. И первым в этой коллекции уязвимых инструментов будет DNS.

Запросы к системе доменных имен предшествуют практически каждой интернет-транзакции. Журнал моих запросов DNS в плане содержащейся в нем информации, пожалуй, эквивалентен тому, чем был для предыдущего поколения список набранных телефонных номеров. Пусть журнал транзакций DNS и не содержит информацию о конкретных действиях в сети, но в нем регистрируется то, к каким сайтам я обращался – а зачастую этого достаточно, чтобы создать весьма точный профиль того, чем конкретно мы занимаемся в Интернете. Нередко отмечают, что метаданные такого вида даже полезнее для различных видов анализа, поскольку не загромождены описаниями отдельных действий.

Не только спецслужбы полюбили стоять у нас за плечом и подсматривать, что происходит на наших экранах. Появилось множество продуктов и услуг, нацеленных на индивидуального пользователя и стремящихся построить всеобъемлющий профиль его желаний и потребностей. Хэл Вариан (Hal Varian), главный экономист Google, однажды заметил, что надоедливую рекламу отличает от своевременной подсказки лишь уровень точности и актуальности данных о пользователе. Потому неудивительно, что многие компании строят подобные профили для своей клиентской базы просто по работе. Дошло до того, что во многих случаях на стоимость чистых активов компании больше влияет не ценность и прибыльность ее продуктов и услуг, а масштаб собранной клиентской базы, ее общая покупательная способность и точность информации о ней. И с этой точки зрения поток запросов DNS – настоящий Клондайк.

DNS – находка для шпиона

DNS невероятно болтлив, и доступ к его данным может получить буквально кто попало!

Чтобы преобразовать новое имя, например, *www.example.com*, резолвер DNS сначала запрашивает IP-адрес имени *www.example.com* у корневых серверов имен. Очевидно, корневой сервер не может ответить на этот запрос, поэтому он в ответ выдает список серверов имен, ответственных за домен .com. Затем резолвер снова отправляет запрос IP-адреса для имени *www.example.com*, на этот раз серверу имен .com – и снова получает непрямой ответ, означающий, что сам сервер не знает адреса, но за адреса домена example.com отвечают такие-то и такие-то серверы имен, и адресовать запрос нужно им. Теперь резолвер может направить тот же самый запрос серверу, отвечающему за домен example.com – и, возможно, наконец-то получит от него в ответ адрес *www.example.com*. Но у этой горы запросов есть и неприятный побочный эффект. Корневой сервер имен, сервер имен .com и сервер example.com теперь знают, что меня

интересует имя *www.example.com*, и они наверняка ведут журнал подобных запросов. Откуда мне знать, общедоступен он или закрыт? Кто и как анализирует журнал, какие выводы делают из этих данных? Нет ответа.

А может быть, ситуация еще хуже: ведь приложение, с которым я работаю, например, браузер, как правило не выполняет трансляцию имен DNS само. Оно для этого обращается к операционной системе, например в форме запроса *gethostbyname()*. А ведь ОС тоже может вести журнал подобных запросов. Получается, что мой браузер и моя ОС осведомлены о моих действиях. Платформа операционной системы, как правило, не содержит автономного резолвера DNS, а настроена на вызов удаленного резолвера. Обычно такой рекурсивный резолвер предоставляется интернет-провайдером. Все это хорошо и замечательно, но, выходит, мой провайдер тоже знает всю мою историю обращений к DNS.

Дальше – больше. Провайдер, чтобы не связываться с поддержкой полномасштабного сервера DNS, может транслировать запросы другому рекурсивному резолверу, т.е. еще одной стороне. Как правило, подобные пересылки влекут за собой потерю атрибуции, так как пересылаемые запросы не содержат моих идентификационных данных. Но если резолвер использует опцию EDNS Client Subnet (RFC 7871, https://datatracker.ietf.org/doc/rfc7871), тогда пересылаемые запросы сохраняют ряд важных данных о моей локальной сети.

Из этого примера видно, что о моем интересе к сайту *www.example.com* узнает множество посторонних лиц.

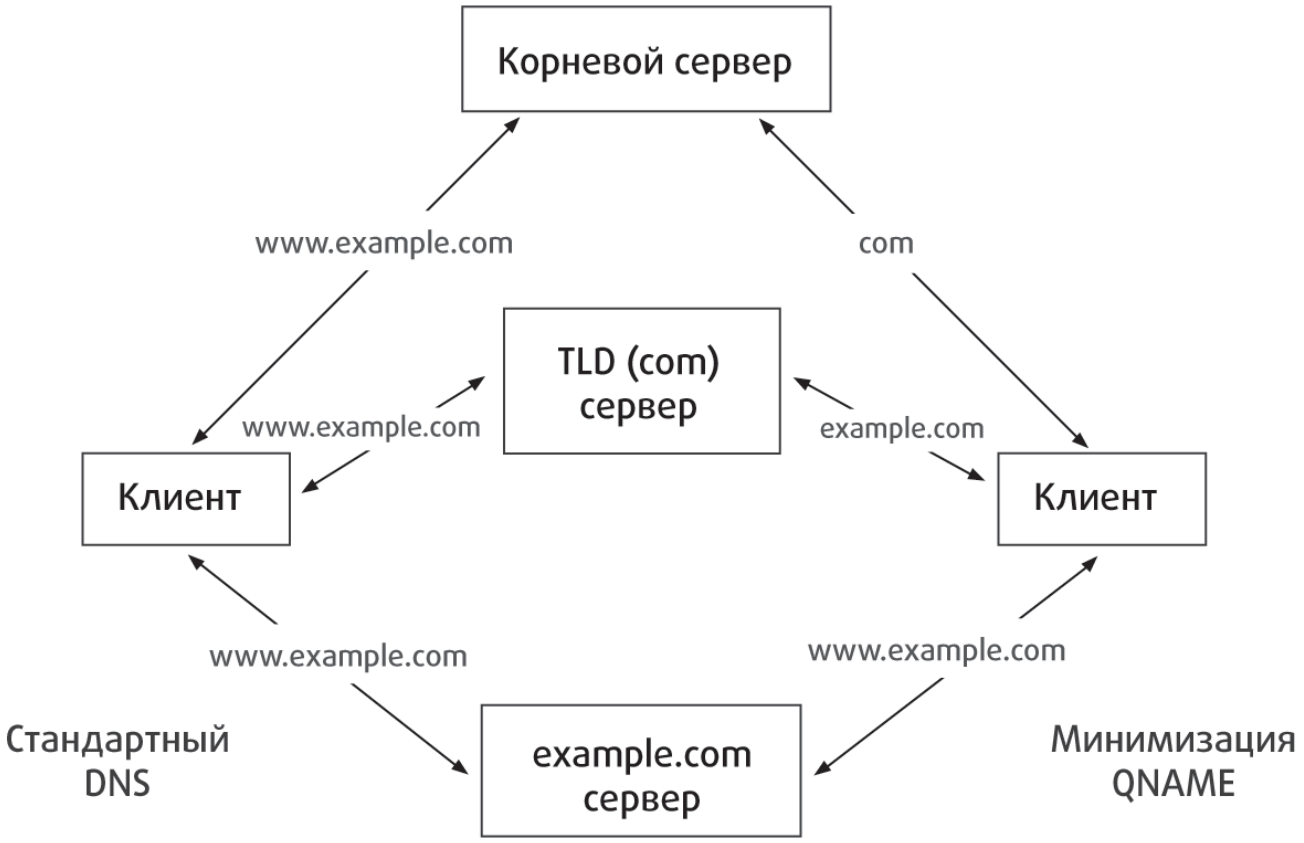
Все эти запросы DNS – огромная куча данных даже по меркам нынешнего информационного века. Еще в апреле 2015 года Google сообщил, что его серверы DNS выдают около 400 миллиардов ответов в сутки (https://webmasters.googleblog.com/2014/12/google-public-dns-and-location.html), а по другим сведениям, Google обрабатывает примерно 12% общей нагрузки DNS (http://stats.labs.apnic.net/dnssec/XA). Получается, что на тот момент в мире генерировалось порядка трех триллионов запросов DNS. С тех пор эта цифра точно не стала меньше.

Мало того, что DNS беспардонно делится информацией о действиях пользователя с кем попало – он еще и передает ее открыто. Запросы DNS и ответы на них не шифруются, просто сидят на порту 53 для UDP и TCP. Запросы DNS легко можно перехватить, а если не используется DNSSEC – и подсунуть в поток данных фальшивые ответы, а клиент ничего не заметит. В некоторых странах перехват и подмена DNS уже стали обычным делом. Другие обратились к перехвату и блокировке DNS, пытаясь решить проблемы, связанные с перегрузкой IP-адресов при виртуальном веб-хостинге.

Можно ли «научить» DNS здоровой осторожности?

В последние годы IETF, наконец, занялась приватностью DNS, и появились предложения по его доработке, с тем чтобы лишить шпионов и цензоров всех мастей их любимого инструмента. Рассмотрим эти инициативы подробнее.

Рис. 1. Предлагаемая схема минимизации имен запросов.



Минимизация QNAME

В рабочей группе DNS Operations возникло предложение минимизировать имена запросов DNS, в результате чего появилась спецификация QNAME Minimisation (RFC 7816, https://datatracker.ietf.org/doc/rfc7816, март 2016 г.). В этом документе говорится: «Минимизация QNAME исходит из того принципа, что чем меньше рассылается данных, тем меньше возникает проблем с их утечкой» – на мой взгляд, более чем разумная позиция.

В вышеприведенном примере запрос к корневым серверам для получения IP-адреса *www.example.com* содержит два лишних элемента информации, а именно полное доменное имя и тип запроса. Разумнее и безопаснее было бы запросить у корневых серверов имен записи NS для домена .com, не делясь информацией, которая корневым серверам вообще не нужна. Аналогично, у серверов имен .com лучше было бы запрашивать список серверов имен для домена *example.com* и так далее (см. рис. 1).

Минимизация QNAME в плане эффективности ничем не хуже передачи полного имени запроса, да и возможность использовать кэшированные данные не страдает. Она выявила ряд несоответствий при обработке т.н. пустых нетерминальных доменных имен (empty non-terminal domain names), но сам подход реализуется надежно и станет хорошим шагом к тому, чтобы положить конец разбазариванию информации. Никаких изменений на серверах DNS не требуется, а любой резолвер, реализующий этот метод, предоставит своим пользователям преимущества защиты их данных.

Одними из первых резолверов DNS, реализовавших минимизацию QNAME, стали Knot DNS Resolver, разработанный CZNIC (https://www.knot-resolver.cz), и Unbound (https://www.unbound.net) (начиная с версии 1.5.7, хотя, как я понял, в реализации преобразователя Unbound минимизация QNAME по умолчанию отключена).

DNS по безопасному каналу

Минимизация имен запросов DNS решит лишь часть проблем – ведь в DNS вообще ничего не шифруется. Благодаря такой открытости DNS, прослушивать, перехватывать и подменять его данные невероятно просто. Этой проблемой занимается рабочая группа DPRIVE (https://datatracker.ietf.org/wg/dprive/about/) в составе IETF, пытаясь найти способы защитить обмен запросами и ответами DNS между клиентом и резолвером.

Здесь главная проблема – обеспечить безопасность протокола преобразования имен DNS. Причем для обеспечения безопасности нужно решить две задачи. Во-первых, требуется защитить транзакции DNS от прослушивания, т.е. зашифровать трафик DNS. А во-вторых, клиенты DNS должны отправлять запросы только своему резолверу DNS и проверять, что полученный ответ действительно пришел от нужного резолвера. Таким образом клиент сможет удостовериться в подлинности транзакции DNS, а попытки перехвата будут для него легко различимы.

DNS поверх TLS

У нас уже есть сеансовый сервис общего назначения, способный обеспечить такую безопасность на уровне сеанса, а именно протокол TLS (Transport Layer Security). TLS вырос из более раннего протокола SSL (Secure Socket Layer), разработанного Netscape в 90-е годы.

Надо признать, что сочетание TLS и DNS в одной фразе вызывает довольно бурную реакцию в сообществе DNS. По вопросу использования TCP вместо UDP в качестве основного транспортного протокола для DNS, а не резервного варианта для больших ответов, было сломано множество копий. Утверждалось, что усилия по поддержке соединения TCP значительно затруднят для сервера обработку больших объемов запросов, а дополнительная задержка на первоначальное «рукопожатие» негативно отразится на пользователе. Другая сторона оперировала следующими аргументами: «Веб и так уже используется, в основном, как служба коротких транзакций, и веб-серверы неплохо справляются с подобной нагрузкой. Кроме того, применение TCP – эффективное лекарство от различных злоупотреблений, эксплуатирующих уязвимость UDP к спуфингу исходных адресов».

Спецификация DNS поверх TLS (RFC 7858, https://datatracker.ietf.org/doc/rfc7858, май 2016 г.) довольно проста: транспортная служба, обеспечиваемая TLS, фактически та же, что и у TCP, с тем отличием, что порт прослушивания на сервере – TCP 853, а не 443.

Недостатком TLS является необходимость выполнить трехэтапное «рукопожатие» TCP для создания сеанса, а затем передачу аутентификационных данных TLS для создания защищенного сеанса. В TLS 1.2 это означает, что перед тем как запрос клиента поступит на сервер, должно пройти три интервала передачи данных с клиента на сервер и обратно (Round Trip Time, RTT). В более новой версии TLS 1.3 планируется улучшить положение, избавившись от одной RTT, но все равно это будет куда медленнее UDP и, скорее всего, увеличит нагрузку на серверы DNS за счет необходимости поддерживать сеансы.

Есть, однако, одно изменение, которое позволило бы устранить существенную, если не большую часть дополнительной нагрузки – вариант с повторным использованием сеансов TLS. В спецификации DNS поверх TLS предлагается именно это: «Чтобы свести к минимуму задержку, клиентам СЛЕДУЕТ направлять несколько запросов в сеансе TLS конвейерно». Для обмена данными между клиентом и рекурсивным резолвером повторное использование сеанса имеет смысл, но при обмене данными между авторитетным сервером имен и клиентом, который сам выполняет преобразование DNS, это может быть малореально.

Также интересно предложение использовать выделенный порт TCP. Если надо замаскировать шифрованный трафик DNS и затруднить блокировщикам его обнаружение, то напрашивается вариант пустить DNS поверх TLS через порт 443 (по крайней мере, я бы так и сделал!). А зашифрованный трафик через ничем больше не занятый порт TCP просто кричит: «Вот он я, блокируй – не хочу!» - и тогда будет гораздо легче заставить вас отказаться от шифрования DNS. Куда логичнее пустить безопасный трафик

DNS через активно используемый порт TCP 443, где его будет значительно труднее выделить.

В ближайшие месяцы DNS поверх TLS будет реализован для устройств Android, так что можно ожидать некоторого повышения приватности DNS в этом аспекте.

Узнать больше о нынешнем состоянии клиентов и серверов, поддерживающих DNS поверх TLS, можно по адресу https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status.

Проблема этого варианта в том, что хотя обмен данными между тупиковым резолвером и выбранным рекурсивным резолвером шифруется, ваш рекурсивный резолвер все равно оказывается в курсе всего, что вы делаете по DNS. От атак на канал это защитит, но что касается ситуации на другом конце канала, тут остается только уповать на порядочность и квалификацию хозяев сервера.

DNS поверх DTLS

TCP не всегда будет оптимальным способом создать безопасный канал для DNS. TCP пытается доставлять данные последовательно, а в приложении, ориентированном на сообщения, потеря сообщения в TCP задержит доставку всех последующих до тех пор, пока TCP не исправит потерю данных и не передаст пропавшее сообщение. Эта особенность TCP может привести к неприемлемому возрастанию нагрузки при передаче сообщений по типу датаграмм: одна потеря, как вредный или нерасторопный покупатель, будет задерживать всю очередь. Для защиты приложений на основе UDP лучшим вариантом мог бы оказаться IPSEC, но IPSEC – функция ядра, а не модуль прикладного уровня, и его семантика применяется на уровне IP, а не в качестве атрибута транспортного протокола. Это затрудняет реализацию IPSEC в приложениях и развертывание криптографических функций в пространстве пользователя.

Альтернативный вариант защиты транспорта DNS – внедрение безопасного уровня сеанса в среду передачи датаграмм. На этом и построен новый протокол DTLS, представляющий собой адаптацию функции TLS, которая может обеспечить приложению функцию доставки по типу датаграмм, не требующую надежного транспортного сервиса. DTLS может восстанавливать потерю пакетов и выполнять переупорядочение, но нетерпим к фрагментации пакетов UDP. Он построен по образцу TLS 1.2 и пытается немного снизить негативное воздействие от использования TLS на качество работы DNS, особенно по сравнению с вариантом «DNS поверх TLS поверх TCP». Главное отличие – необходимость первоначального рукопожатия DTLS для того, чтобы создать общее состояние шифрования, и применение файлов cookie, чтобы повторно использовать это состояние на протяжении нескольких отдельных взаимодействий «запрос-ответ».

Применение DNS в его нынешнем варианте поверх UDP отличается тем, что накладные расходы на обслуживание общего состояния нагружают каждую отдельную транзакцию по минимуму, в результате чего сервис оказывается очень надежным и оперативным. DNS поверх DTLS пытается, насколько возможно, сохранить эту простую модель обмена датаграммами «запрос-ответ», но при этом сделать так, чтобы клиент использовал шифрование, основанное на предложенных сервером и проверенных сертификатах (RFC 8094, https://datatracker.ietf.org/doc/rfc8094, февраль 2017 г.).

DTLS нетерпим к фрагментации IP, поэтому реализация DNS поверх DTLS по структуре своей сходна с использованием флага TC в реализации DNS поверх UDP: если размер ответа превосходит MTU маршрута, то сервер должен выдать сокращенный ответ и установить флаг TC, чтобы просигнализировать клиенту о необходимости повторить запрос по TCP. Цель такого поведения в случае DTLS в следующем: если сервер DNS поверх DTLS выдает ответ длиннее, чем оценка MTU локального маршрута, то сервер должен в ответе установить флаг TC, а клиент интерпретирует это как инструкцию повторить запрос по DNS поверх TLS.

Спецификация DTLS содержит любопытную оговорку: «Это решение DTLS рабочая группа DPRIVE сочла подходящим вариантом для использования в случае, если метод на основе TLS, описанный в RFC7858 (https://datatracker.ietf.org/doc/rfc7858), обнаружит проблемы при внедрении. На момент написания спецификации ожидается, что RFC7858 будет внедрен, а потому настоящая спецификация задумана, главным образом, как резервная».

Похоже, сами разработчики не очень-то верят в DTLS: разумно сделать вывод, что на сей момент интерес к DNS поверх DTLS невелик, и спецификация DTLS разработана, скорее, не для широкомасштабного применения, а в качестве формальности.

> «Минимизация QNAME исходит из того принципа, что чем меньше рассылается данных, тем меньше возникает проблем с их утечкой» – на мой взгляд, более чем разумная позиция.

Безопасный DNS поверх JSON

И DNS поверх TLS, и DNS поверх DTLS просто заменяют транспортный протокол, никак не трогая формат запросов и ответов. Но, разумеется, никто не объявлял формат DNS неприкасаемым, а потому есть и другие методики, основанные на новом представлении запросов и ответов DNS.

Сервер по адресу https://dns.google.com выполняет функцию трансляции поверх TLS через порт 443, передавая результаты в формате структур данных JavaScript Object Notation (JSON). Эту реализацию легко превратить в альтернативную форму *gethostbyname()* для приложения, заменяя обычный запрос DNS выбор-

кой веб-объекта. Преимуществом для вызывающего станет некий уровень защиты от прослушивания третьими сторонами, потенциального вторжения и цензуры… хотя непонятно, о какой «защите» может идти речь, если вы оповещаете о своих действиях DNS-серверы Google!

Однако, чтобы проиллюстрировать, как приложение может использовать такой сервис непосредственно, обходя перехват как со стороны платформы, так и локального DNS, приведу пример скрипта Python, который устанавливает безопасный сеанс с этим сервисом Google:

```
#!/usr/bin/python
import json, requests

url = "https://dns.google.com/
resolve"
params = dict(
    name='www.potaroo.net',
    type='A',
    dnssec='true'
)

resp = requests.get(url=url,
params=params)
data = json.loads(resp.text)

print(data[u'Answer'][0]
[u'data'])
```

Этот метод может оказаться полезным, так как опасения об утечке данных DNS нельзя ограничивать только внешними формами слежки и перехвата. «Адекватно осторожное» приложение не будет использовать службу трансляции имен DNS, предоставленную платформой, поскольку тогда запросы DNS приложения попадут в неконтролируемую среду, где могут регистрироваться платформой и другими приложениями. В этом случае приложение не выполняет трансляцию DNS и проверку DNS само: оно использует безопасный канал связи со службой трансляции имен Google по соединению TLS. Приложение может быть в некоторой степени уверено в том, что не допускает локальной утечки данных DNS, и что (при включенной проверке DNSSEC) получаемые ответы с известной степенью надежности достоверны, при условии, что само преобразуемое имя подписано по DNSSEC.

Отправка запросов по безопасному каналу на очень загруженный рекурсивный резолвер – а вряд ли найдется резолвер более загруженный, чем общедоступный DNS-сервер Google – имеет еще и то преимущество, что ваши запросы могут затеряться в горе кэшированной информации и тем избежать обнаружения. Если вы не против того, чтобы оповещать Google о своих запросах DNS, то довольно разумно использовать безопасный доступ к рекурсивному DNS-резолверу, который стремится к точности, целостности и полноте в выполнении своих задач. Такой безопасный канал гораздо труднее обойти и прослушать поток запросов.

Если же такой вариант вас не устраивает, есть и другой: вернуть трансляцию имен на свою платформу или даже в приложение, используя такие инструменты, как GetDNS (https://getdnsapi.net/). Здесь, правда, возникнет другая проблема: да, вы не доверяете чужому рекурсивному резолверу и ваши запросы напрямую передаются на ответственные серверы имен, но зато вы опять используете незашифрованный DNS – а к тому же теряете преимущество в быстродействии из-за общего кэша DNS. Возможно, лучше использовать безопасный канал к рекурсивному преобразователю, которому вы доверяете, но выполнять проверку DNSSEC самостоятельно.

DNS поверх HTTPS

Теперь мы можем обратиться к стандартизационной работе в IETF, где рабочая группа DOH пытается стандартизировать DNS поверх HTTPS. В уставе этой рабочей группы записано: «Данная рабочая группа стандартизирует шифрование для запросов и ответов DNS, пригодное для использования в HTTPS. Это позволит системе доменных имен функционировать на некоторых маршрутах, где существующие методы DNS (UDP, TLS [RFC 7857, https://datatracker.ietf.org/doc/rfc7857] и DTLS [RFC 8094, https://datatracker.ietf.org/doc/rfc8094]) столкнулись с проблемами. Данная рабочая группа будет в максимально возможной степени повторно использовать методы, коды ошибок и прочую семантику HTTPS. Применение HTTPS и его существующего PKI обеспечивает целостность и конфиденциальность, а также взаимодействие с общей инфраструктурой и политиками HTTPS».

Какой метод используется здесь?

Новые метки URI для различных схем именования URI сейчас не в моде, и работа DOH не стала исключением. Вместо того, чтобы повторно задействовать префикс «dns:», рабочая группа использует популярный в наше время механизм, а именно хорошо известный URI-путь «.well-known/dns-query». В этой схеме запрос DNS может выглядеть так:

```
:method = POST
:scheme = https
:authority = dnsserver.example.net
:path = /.well-known/dns-query
accept = application/dns-udpwireformat
content-type = application/dns-
udpwireformat
content-length = 33

<33 байта представлены следующим
шестнадцатеричным кодом>
abcd 0100 0001 0000 0000 0000 0377 7777
0765 7861 6d70 6c65 0363 6f6d 0000 0100
01
```

В этой методологии используется существующий двоичный формат DNS по проводу с применением типа данных MIME «application/dns-udpwireformat». При использовании метода GET запрос DNS шифруется по Base64, в то время как метод POST помещает двоичный запрос DNS в тело HTTP-объекта, к которому применяется POST, как в примере выше.

Надо сказать, я не слишком понимаю, в чем тут выгода. Дополнительная оболочка HTTP не добавляет практически ничего, кроме ненужных украшательств – и никаких преимуществ, кроме демонстрации ловкости рук, я тут не вижу! Если все, что нам надо – это упрятать запросы DNS в зашифрованный канал, то в HTTPS этим занимается тот же TLS, а компонент HTTP лишь усложняет задачу. Так может, просто использовать DNS поверх TLS?

Что дальше?

Мы затронули не все аспекты приватности DNS.

Например, есть еще и возможность паддинга (заполнение пустыми данными) пакетов. Даже если содержимое DNS передается по зашифрованному сеансу, есть возможность установить факт обмена данными DNS по размеру пакетов запроса и ответа DNS. Если блокировать такой зашифрованный трафик DNS, то пользователи будут вынуждены передавать данные DNS открыто и подставляться под DNS-атаки. С этим пытается бороться паддинг DNS (RFC7830, https://datatracker.ietf.org/doc/rfc7830, май 2016 г.): можно увеличивать размер запросов и ответов DNS, добивая их переменным количеством байтов, чтобы нельзя было отлавливать зашифрованный трафик по длине. Однако, хотя эта спецификация описывает, как добавлять мусорное содержимое, она не рекомендует никакой конкретной политики паддинга. Этой темой сейчас занимается IETF, и рабочая группа DRPIVE вырабатывает новую спецификацию, ориентированную на политики (текущий рабочий документ носит имя draft-ietf-dprive-padding-policy), чтобы дать полезные рекомендации в части политик паддинга, которые пригодятся клиентам DNS.

Еще один аспект, заслуживающий рассмотрения, это взаимодействие между рекурсивным резолвером и авторитетным сервером имен. До сих пор основные усилия по защите передачи DNS были сосредоточены на канале, ведущем от оконечного клиента к рекурсивному резолверу, а ведь канал от преобразователя к серверу имен не лишен тех же самых проблем. Недавно в этой сфере появились подвижки (рабочий документ носит имя draft-bortzmeyer-dprive-resolver-to-auth-00): предлагается использовать DANE и возложить на DNS публикацию открытого ключа сервера для запросов DNS поверх TLS. Работа находится еще на ранней стадии и наверняка будет переделываться, но выглядит эта идея достойно.

Паддинг может устранить некоторые очевидные паттерны трафика DNS, которые не сможет скрыть шифрование, но остается еще проблема времени передачи пакетов: оно тоже демаскирует обмен данными DNS. Ведутся разговоры о том, не стоит ли добавлять пакеты-«пустышки» в потоки запросов и ответов, чтобы лучше замаскировать паттерны коммуникации DNS. Пока неясно, что из этого получится, но если ответом на шифрование сеансов DNS действительно станет блокировка шифрованного трафика DNS, то идея добротной маскировки этого трафика наберет популярность среди пользователей.

Состояние дел с приватностью DNS

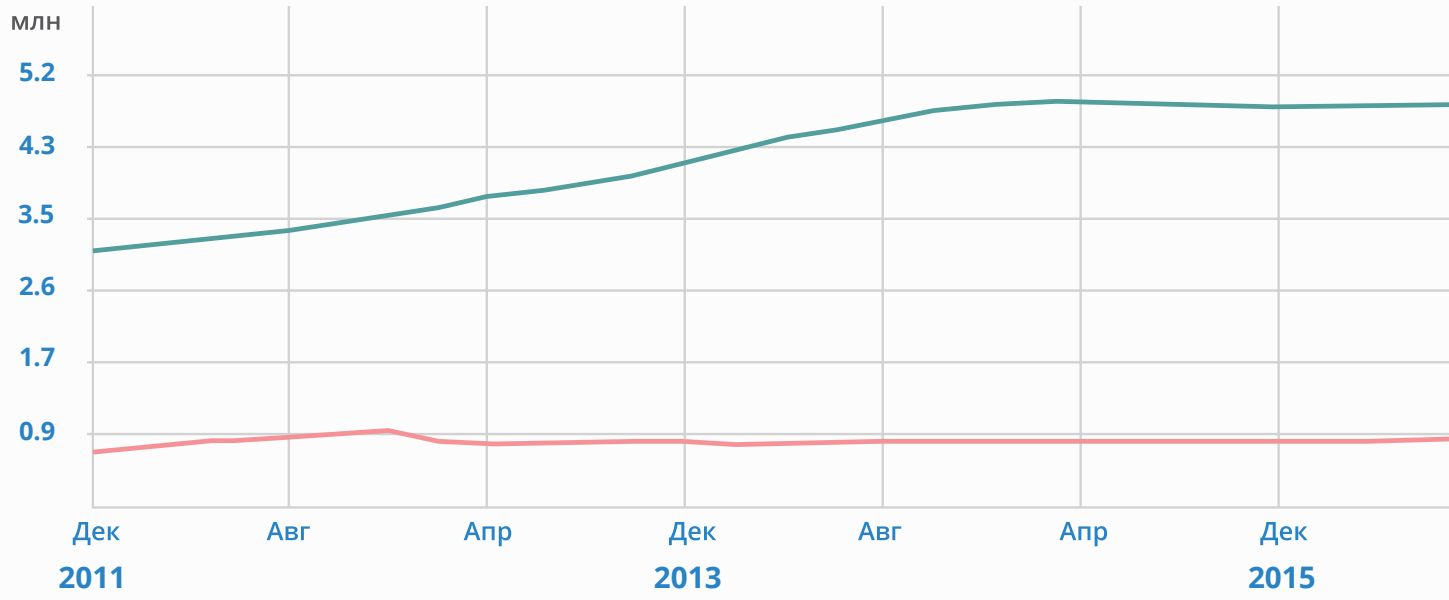
Да, в наши дни открытость DNS невероятно облегчает его прослушку, перехват и подмену данных; но отчаиваться рано – прилагается много усилий к тому, чтобы создать среду DNS, которая защищала бы конфиденциальность и целостность данных.

Минимизация имен запросов позволит значительно сократить уровень утечки информации DNS. А передача запросов и ответов DNS по безопасному каналу затруднит посторонним лицам прослушку и перехват пакетов DNS в пути.

Если приложения начнут использовать сервисы, которые инкапсулируют локальный трафик запросов DNS в зашифрованных сеансах TLS, то значительная часть данных DNS, доступных сегодня любому желающему, просто исчезнет из поля зрения. Более того, нынешняя практика выборочной локальной инспекции и вмешательства в процесс преобразования имен DNS станет гораздо более трудной, если вообще возможной.

Если вдобавок ко всему этому еще и широко распространится DNSSEC, облик Интернета существенно изменится. Само собой, попытки цензуры Интернета никуда не денутся – равно как и практика мониторинга и слежки в сети. Но если все мы решим всерьез заняться приватностью и безопасностью DNS, он перестанет быть тем, чем является сейчас – исключительно простым и дешевым инструментом для этих неблаговидных целей.

Источник: DNS privacy, Geoff Huston

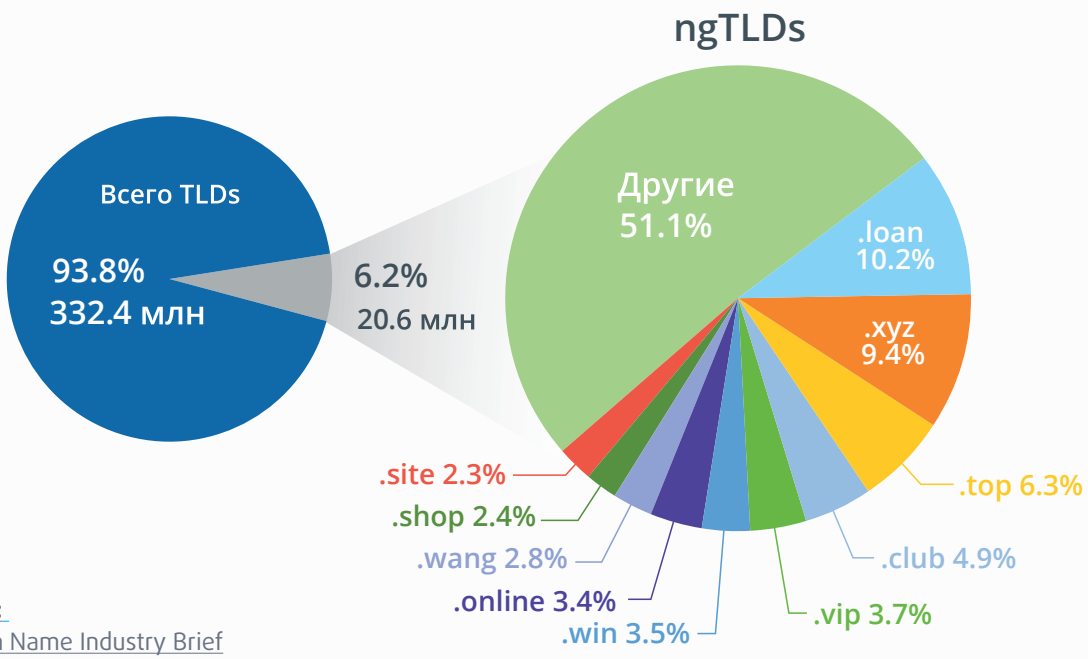


Источник:
https://statdom.ru/

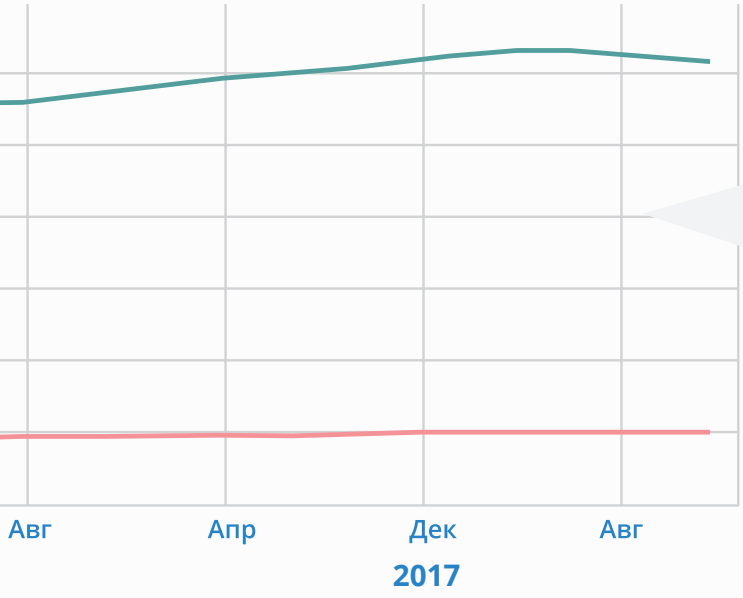
Использование доменов .su, .ru, .рф за февраль 2018 года

- Веб-перенаправление
- Веб-сайт
- Веб-приложение / одностраничный сайт
- Известные парковки
- Только почта

Общее количество доменов TLDs меньше, чем ngTLDs



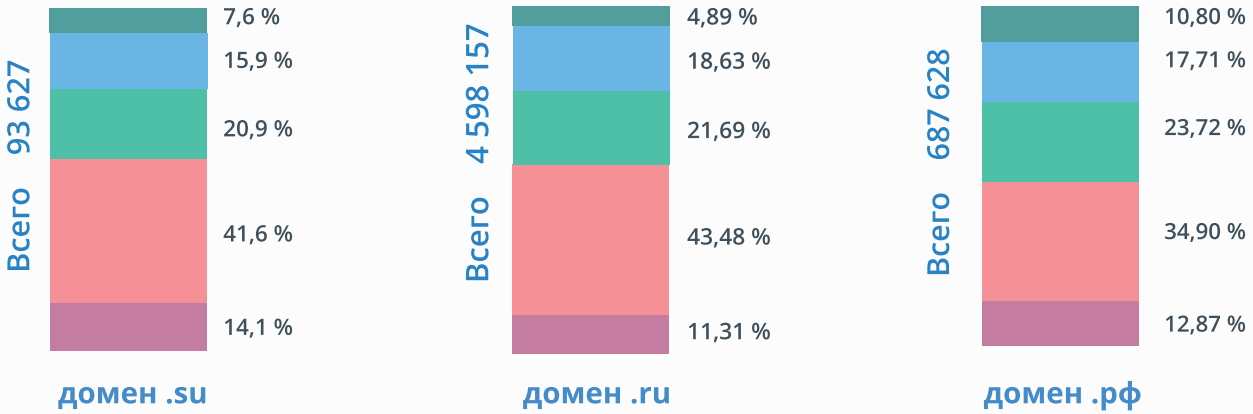
Источник:
The Domain Name Industry Brief



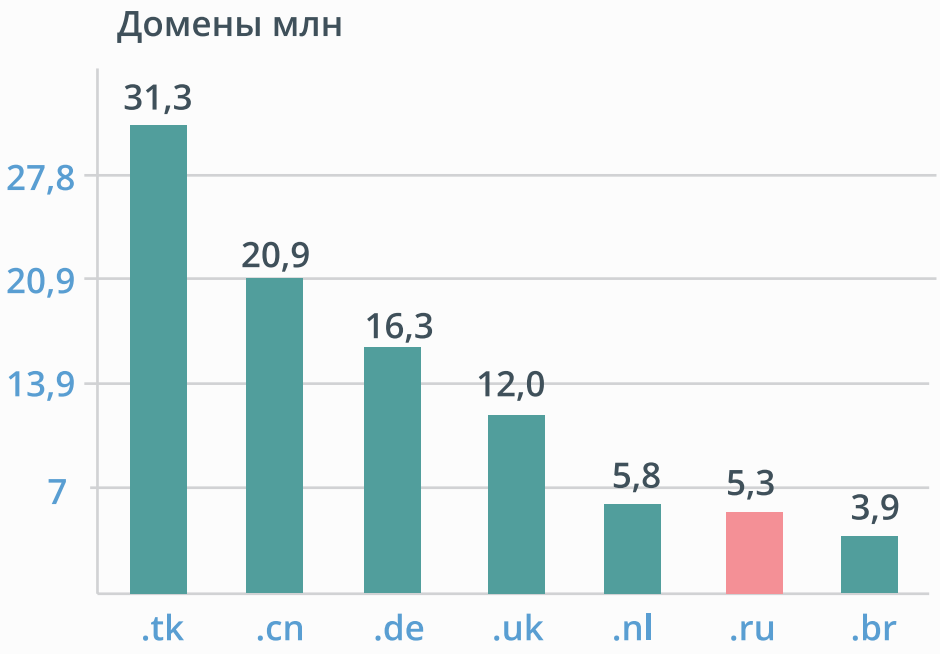
Общее число доменов .ru, .рф с декабря 2010 года по декабрь 2017 года

.РФ
.RU

Источник:
https://statdom.ru/, Общее число доменов



Мировая статистика



Источник:
https://statdom.ru/

DNS и anycast: решения и проблемы

Павел Храмцов

Устойчивость системы DNS, ее надежность, а также достоверность получаемой из DNS информации чрезвычайно важны для функционирования современного Интернета. Одним из таких механизмов повышения надежности является построение DNS-anycast-облаков. Тема реализации сервиса DNS на основе технологии anycast обширна. Реализация DNS-облаков требует глубокого анализа DNS-статистики, продуманных инженерных решений и высокой квалификации обслуживающего персонала. Тем не менее, на данный момент anycast – это наиболее стабильное и надежное решение для построения высоконагруженных DNS-сервисов, к которым предъявляются высокие требования по устойчивости и надежности.

Система доменных имен (Domain Name System - DNS) имеет критически важное значение для современного Интернета. Мало кто помнит IP-адреса сервисов поиска «Яндекса» (5.255.255.70, 77.88.55.80, 77.88.55.70, 5.255.255.80), например. Однако все прекрасно помнят доменное имя yandex.ru.

DNS, придуманная для облегчения именования адресов электронной почты, в настоящее время стала одним из важнейших инфраструктурных сервисов. Обращение к системе DNS всегда предваряет любое другое обращение к информационным ресурсам Сети, будь то сайты World Wide Web, социальные сети, потоковые сервисы или электронная почта.

Устойчивость системы DNS, ее надежность, а также достоверность получаемой из DNS информации чрезвычайно важны для функционирования современного Интернета. Одним из таких механизмов повышения надежности является построение DNS-anycast-облаков.

От серверов к облакам

Давайте посмотрим на стандартный вывод утилиты dig для домена .ru:

```
ru.     345600  IN  NS  f.dns.ripn.net.
ru.     345600  IN  NS  a.dns.ripn.net.
ru.     345600  IN  NS  b.dns.ripn.net.
ru.     345600  IN  NS  d.dns.ripn.net.
ru.     345600  IN  NS  e.dns.ripn.net.
```

Из него видно, что за поддержку домена .ru отвечают пять серверов доменных имен. Каждому из них назначены IP-адреса форматов IPv4 и IPv6:

```
a.dns.ripn.net.   193.232.128.6
                  2001:678:17::193:232:128:6
b.dns.ripn.net.   194.85.252.62
                  2001:678:16::194:85:252:62
d.dns.ripn.net.   194.190.124.17
                  2001:678:18::194:190:124:17
e.dns.ripn.net.   193.232.142.17
                  2001:678:15::193:232:142:17
f.dns.ripn.net.   193.232.156.17
                  2001:678:14::193:232:156:17
```

А теперь проведем следующий эксперимент: запросим список серверов доменных имен домена .ru из трех удаленных мест, скажем, из Франкфурта (Amazon), Орегона (Amazon, Западное побережье США) и Москвы (Beeline). Обращаться будем к одному и тому же авторитетному серверу доменных имен f.dns.ripn.net. А также посмотрим на расстояния между этими точками в терминах времени отклика от DNS-серверов, установленных в этих точках[1]. Измерения времени отклика приведены в таблице 1.

Если принять простое топографическое представление расстояний между точками измерения, то f.dns.ripn.net должен располагаться где-то на Карибских островах.

Однако если задать в команде dig опцию +nsid[2], то можно увидеть нечто большее, чем время отклика, а именно – идентификатор авторитетного сервера (таблица 2).

Таблица 1 **Время отклика по при запросе списка записей NS при обращении к серверу f.dns.ripn.net (ms) утилитой dig**

	f.dns.ripn.net	Орегон (США)	Франкфурт	Москва
f.dns.ripn.net		X	X	X
Орегон	223		165	X
Франкфурт	159	164		X
Москва	288	442	54	

Таким образом, мы увидели два любопытных момента:

- под одним именем и одним адресом «скрываются» два разных сервера;
- география отвечающих серверов не согласуется с простыми географическими представлениями, а определяется топологией сети и политиками маршрутизации провайдеров (Internet Service Provider - ISP).

Назначение одного IP-адреса (а в нашем случае и одного имени) многим хостам в данном случае определяется технологией **anycast**, которая применяется при реализации поддержки домена .ru.

Домен .ru поддерживают не пять серверов, а пять групп серверов. Каждой группе соответствует свое имя (в дальнейшем мы будем их называть по первым буквам имени: a, b, d, e, f). Все серверы в группе имеют одинаковые IP-адреса.

Запросы от резолверов при обращении за информацией о домене .ru в общем случае направляются на ближайшую (в смысле времени отклика) группу серверов, а в ней, соответственно, на ближайший (в смысле длины маршрута) сервер из группы. Группу DNS-серверов мы будем называть anycast-облаком.

Вообще говоря, когда рассуждают об anycast в DNS, то речь идет не столько о DNS, сколько о маршрутизации и требованиях к сервису, для которого устанавливаются anycast-маршруты.

Быть ближе к народу

Если коротко, то при технологии anycast нескольким географически распределенным серверам назначается один и тот же IP-адрес (IPv4 или IPv6), называемый anycast-адресом. Когда какой-либо хост отправляет пакеты (датаграммы) на anycast-адрес, система маршрутизации Интернета выбирает, а Сеть отвечает за кратчайший наилучший маршрут к этому адресу. Таким образом обмен трафиком будет происходить с наиболее близким (в терминах протокола маршрутизации BGP) к клиенту сервером доставки пакетов как минимум одному и, даже наиболее предпочтительно, только одному из серверов, которые могут получить эти пакеты на anycast-адрес[3].

Основная идея такого подхода состоит в том, чтобы не выбирать из списка наиболее подходящий сервер вручную, а положиться на выбор системы маршрутизации.

Если применять эту идею к DNS, то она состоит в том, чтобы разработать и развернуть сеть DNS-серверов в районах, которые не покрывались ранее сервисом DNS, и таким образом сократить время отклика на запросы резолверов в этих районах[4].

Сервис, для которого предполагается применять anycast, должен отвечать определенным требованиям:

- anycast может быть реализован только на стабильном списке адресов;
- маршруты к этому списку могут быть анонсированы из различных физически (топологически) разнесенных мест;
- для реализации anycast наилучшим образом подходят так называемые stateless протоколы.

Для сервиса DNS все перечисленные требования к реализации сервиса хорошо подходят.

В своей массе запросы к DNS используют транспорт UDP, т.е. мы имеем дело со stateless протоколом. Кроме того, при этом большинство запросов вмещаются в один DNS-пакет, что, собственно, не требует поддержания канала между клиентом и сервером в течение длительного времени.

Список IP-адресов авторитетных серверов стабилен и задан в файле описания зоны. Изменения списка возможны, но они происходят не чаще, чем происходит изменение адресных записей в соответствующих файлах описания зон доменов.

Здесь следует заметить, что когда речь заходит об anycast для DNS, то, как правило, имеют в виду либо группы серверов, которые поддерживают корень DNS, либо группы серверов, поддерживающих национальные домены (country code top level domains – ccTLD), либо домены верхнего уровня общего назначения (General Top Level Domains – gTLD). Политика маршрутизации автономных систем для этих серверов обычно

Таблица 2 **Идентификатор авторитетного сервера для различных регионов**

Местоположение	Орегон	Франкфурт	Москва
Идентификатор сервера	tau-sin.ripn.net (Сингапур)	tau-sin.ripn.net (Сингапур)	tau-spo.ripn.net (Сан-Паулу)

довольно стабильна. Технологии типа fastflux для серверов, поддерживающих эти домены, также не используется.

При реализации маршрутов к узлам anycat-облака могут быть использованы два разных способа объявления маршрутов: анонсирование «глобальных» узлов и анонсирование «локальных» узлов.

«Глобальные» узлы анонсируются таким образом, что они могут обслуживать резолверы, размещенные в любой точке Интернета. Как правило, «глобальные» узлы подключены к нескольким интернет-сервис-провайдерам. Обычно глобальный узел устанавливается в сетях глобальных или крупных региональных провайдеров.

«Локальные» узлы анонсируются только определенной группе провайдеров и не должны быть доступны «всему Интернету». Для анонсирования таких узлов могут быть применены технологии ограничения «видимости» маршрутов к таким узлам[5]. «локальные» узлы обычно обслуживают локальное сообщество пользователей и размещаются в точках обмена трафиком (IX).

Со временем список задач DNS, которые можно решать в рамках технологии anycat, постепенно расширился до:

1. Распределение трафика среди множества серверов.
2. Противодействие DDoS-атакам на DNS-инфраструктуру за счет распределения трафика атаки.
3. Локализации DDoS-атак вокруг «локальных» DNS-узлов.
4. Сокращение времени отклика.
5. Сокращение списка записей NS (Name Service) в файле описания зоны при фактическом увеличении количества серверов, что положительно сказывается на размер DNS-пакета.
6. Обслуживание максимального количества запросов резолверов при соблюдении соглашений об уровне предоставления сервиса (Service Level Agreement – SLA).

Это далеко не весь перечень задач, для решения которых можно использовать anycast.

Зри в корень: противодействие DDoS-атакам

Устойчивость системы DNS постоянно испытывается широкомасштабными атаками со стороны хакеров. Anycast – это технологический ответ на такие «испытания».

Первая значимая атака на корневые серверы системы DNS была зафиксирована 21 октября 2002 года[6]. Атаке подверглись все 13 серверов (в то время технология anycast еще не была внедрена). Мощность атаки составила от 50 до 100 Мбит/с на каждую букву[7].

Это был ICMP-флуд (очень большой объем трафика по протоколу ICMP), пакеты TCP SYN и фрагментированные TCP- и UDP-пакеты (т.е. использовались уязвимости транспортного уровня стека протоколов TCP/IP). От этого флуда пострадали девять из 13 корневых серверов.

По результатам разбора атаки протокол ICMP зафильтровали[8], описали атаку, но, главное, в ICANN был создан комитет Security and Stability Advisory Committee (SSAC), который занялся анализом угроз и выработкой рекомендаций по их нейтрализации. К слову, в настоящее время ICMP на многих корневых узлах не фильтруют.

Следующая атака случилась 6 февраля 2007 года[9]. Согласно отчету ICANN, мощность атаки составляла около 1 Гбит/с на один сервер. Атаке поверглись в основном серверы Азиатско-Тихоокеанского региона. Из 13 серверов были атакованы шесть, но только два из них реально имели серьезные проблемы с обслуживанием DNS-запросов (более 95% получили отказ обслуживания). Это были сервер Министерства обороны США (g-root) и сервер ICANN (l-root).

Проблемы на этих серверах возникли из-за того, что администрация серверов еще не внедрила технологию anycast (anycast-облака), которая начала активно применяться после 2002 года. Благодаря заранее проделанной работе по обеспечению безопасной и стабильной работы системы, корень системы DNS в 2007 году был готов принять новые мощные атаки.

Собственно, сама технология anycast была предложена в 1993 году в RFC 1546[10]. Уже в этом документе отмечалось, что DNS прекрасно подходит для развертывания на anycast-адресах из-за особенностей транспортного уровня, где более 80% трафика приходится на UDP.

В апреле 2002, т.е. еще до атаки на корневые серверы, в RFC 3258[11] были даны уточнения и рекомендации относительно развертывания сервиса DNS на anycast-адресах. Документ специально не содержал в названии термин «anycast», чтобы подчеркнуть тот факт, что никаких специальных усилий по выделению отдельного anycast-пространства адресов и особенной маршрутизации не требуется по сравнению со стандартными процедурами, ориентированными на unicast.

Следующая значимая атака была проведена 30 ноября – 1 декабря 2015 года на корневые серверы системы DNS[12]. Мощность атаки составляла 5 миллионов запросов на каждый корневой сервер (букву). Существенные задержки обслуживания и отказы обслуживания по timeout наблюдались у корневых серверов b-root, c-root, g-root, и h-root.

Атака на корень была реализована за счет эффекта усиления на резолверах (кэширующих DNS-серверах ISP) и подмены адресов источника в UDP-пакетах (spoof). Наиболее устойчиво себя ощущали «буквы» (корневые серверы), для развертывания которых использовалось решение DNS-anycast-cloud.

Таким образом, во всех последних случаях атак на корень системы DNS технология anycast помогла справиться с

атаками. Но как показали последующие события, anycast не является «универсальной таблеткой» от всех болезней.

«Шагреневая кожа» DNS-сети

21 октября 2016 года DNS-сеть компании DYN подверглась мощной сочетанной атаке со стороны неизвестных хакеров[13]. Анализ атаки показал[14], что для организации атаки использовался ботнет Mirai[15], что по некоторым данным суммарная мощность атаки составила 1,2 Тб/с и что создавали его устройства «интернета вещей» (Internet of Things – IoT). Представители DYN не назвали суммарную мощность атаки, но заметили, что объем DNS-трафика во время атаки увеличился в 10-20 раз.

За обсуждением роли IoT в атаке на DYN на второй план отошел тот факт, что основной объем трафика составили не легитимные DNS-запросы, а флуд. Согласно данным redware.com, набор векторов атаки ботнета Mirai довольно разнообразен (рис. 1).

DNS-трафик определен только в качестве одного из источников нагрузки. Все остальное – это в основном невалидный трафик, который можно и нужно отфильтровать на оборудовании провайдера (ISP) и не допускать до DNS-серверов.

Следует заметить, что фильтрация таких объемов на сетях глобальных провайдеров – это довольно дорогое мероприятие. Если под защиту провайдера ставить каждый DNS-узел в anycast-облаке, то затраты на содержание такой anycast-сети будут впечатляющими.

По этой причине при возникновении сочетанной атаки или атаки с использованием обычного флуда anycast-облака сожмутся до размера защищенных высокопроизводительных узлов или окуклятся в своем регионе, став «локальными» узлами.

Борьбу с формально валидным трафиком будут вести DNS-узлы с плавающими по ситуации лимитами и квотами на обработку запросов. «Размазывание» трафика по anycast-облакам в этом случае не стоит рассматривать как панацею от любого типа атаки. В сети по некоторым оценкам[16], например, в 2014 году было обнаружено 24 миллиона открытых резолверов на домашних маршрутизаторах, которые можно было использовать для генерации трафика в рефлекторных атаках, а также множество IoT-устройств, которые помогут организовать атаки на основе алгоритмов DGA (Domain Generation Algorithm), как это было в случае атаки на DYN.

Дьявол в деталях...

Кроме DDoS существуют другие «подводные камни», которые подстерегают DNS-сеть, реализованную по технологии anycast. Перечислим основные:

- для каждого сервера в узле необходимо предусмотреть два канала подключения (один для предоставления сервиса, а другой для управления);
- определиться со структурой узла (маршрутизатор, DNS-сервер, сервер статистики и прочее, а также определиться с возможностью виртуализации всех этих функций);
- выбрать ПО и «железо», которыми в совершенстве владеет персонал;
- провести настройку компонентов узла, добиваясь максимальной производительности и надежности;
- увеличение количества узлов повышает вероятность ошибок при их (узлов) конфигурации;

Рис. 1. Инструментарий ботнета Mirai.

```
#define    ATK_VEC_UDP        0  /* Straight up UDP flood */
#define    ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define    ATK_VEC_DNS        2  /* DNS water torture */
#define    ATK_VEC_SYN        3  /* SYN flood with options */
#define    ATK_VEC_ACK        4  /* ACK flood*/
#define    ATK_VEC_STOMP      5  /* ACK flood to bypass mitigation devices */
#define    ATK_VEC_GREIP      6  /* GRE IP flood */
#define    ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define  ATK_VEC_PROXY      8  /* Proxy knockback connection */
#define  ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define  ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

- усложняется синхронизация размещенных на серверах файлов зон;
- требуется защита предаваемых по публичной сети файлов зон;
- требуется отлаженная процедура взаимодействия со службами провайдеров, у которых размещены узлы;
- требуется развитая система мониторинга;
- необходимо определиться с уровнем предоставления сервиса и оформить его в виде соглашения (Service Level Agreement);
- требуется определить такое понятие, как «инцидент» и порядок реагирования в случае его наступления.

Наличие двух каналов подключения проистекает из самой сути технологии anycast. Один интерфейс доступен по anycast-адресу, и именно на нем происходит обслуживание запросов резолверов. Второй интерфейс – интерфейс управления и канал передачи файла зоны. Ведь файл зоны нужно передавать по всем хостам облака, а не выборочно какому-то одному. Для этого нужен unicast-адрес.

При выборе параметров интерфейса управления нужно учитывать особенности DNS-сервиса, который предполагается оказывать. Одно дело – передавать большой файл зоны TLD четыре раза в сутки, и совершенно другое дело – каждые 5-10 минут передавать множество небольших файлов зон клиентов, которые к тому же еще подвержены постоянным массовым изменениям.

Структура узла сильно зависит от той производительности, которую ожидают от узла. Если это «глобальный» узел в сети крупного провайдера, то он должен держать высокую нагрузку, и в первую очередь может подвергнуться атаке из Интернета.

«Локальный» узел, напротив, обычно не предполагает высоких нагрузок. Это значит, что его можно виртуализовать. Хотя и из этого правила возможны исключения.

В настоящее время наиболее распространённым ПО, которое поддерживает DNS, являются серверы BIND[17] и NSD[18]. Каждый из них имеет свои положительные и отрицательные свойства. BIND более универсален, NSD в ряде случаев более производителен.

При увеличении количества узлов во избежание ошибок их настройки и конфигурирования необходимо применять автоматизированные системы настройки и конфигурирования, а также развитую систему мониторинга узлов.

Система мониторинга – это вообще отдельный проект, который должен обеспечить независимую оценку работоспособности серверов, узлов и всей системы в целом.

Можно, конечно, воспользоваться чем-то типа RIPE-ATLAS[19]. Но если, скажем, для Европы, где находится множество узлов этой системы, это очевидно хороший вариант, то для Российской Федерации такой вариант подходит не очень – слишком мало узлов и слишком мало бесплатных кредитов, чтобы долго обеспечивать существование широкой сети пробников.

Синхронизация файлов зон – это отдельная большая проблема в распределенной DNS-сети. Спецификации DNS[20] допускают временное расхождение файлов зон на разных серверах. В частности, в рамках параметров SOA-записи, отвечающих за обновление зоны на вторичных серверах.

Следует также заметить, что в настоящее время изменения в содержание зоны сначала вносятся на недоступных из Сети основных авторитетных серверах (hidden-master), а потом распространяются по вторичным серверам. В рамках такого подхода под синхронизацией имеется в виду не расхождение между основным сервером и вторичным, а между вторичными серверами.

Задача может быть усложнена тем обстоятельством, что основных (hidden-master) серверов - из соображений безопасности, надежности и стабильности - может быть несколько. Выгрузка из реестра зоны верхнего уровня может осуществляться поочередно на каждый их них. При больших размерах зон и малом промежутке обновления файла зоны из реестра вероятна ситуация, когда зона на основном сервере обновится раньше, чем предыдущая копия зоны будет доставлена на один из удаленных вторичных серверов. В этом случае ситуацию нужно будет сначала детектировать, а затем и устранить расхождение.

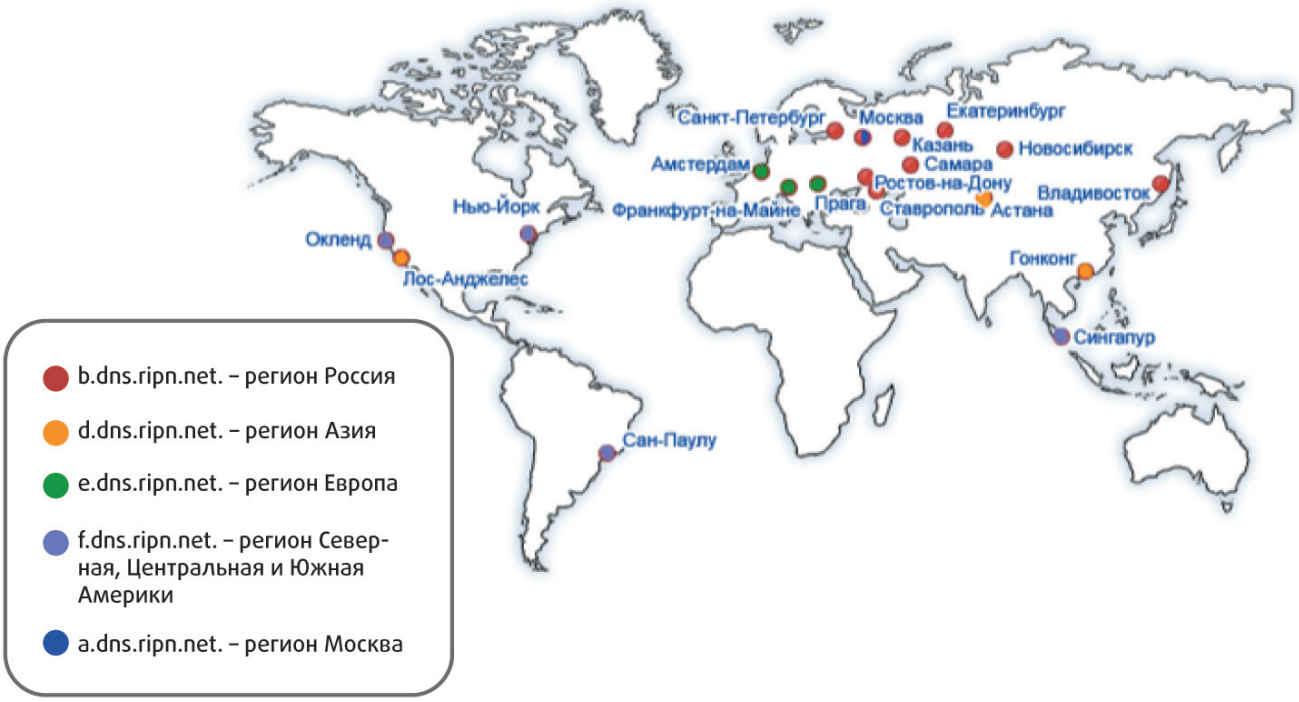
При распространении файлов зоны их следует передавать по защищенным каналам, подписывая. Это нужно для того, чтобы принимающая сторона могла удостовериться в истинности источника информации, а также в том, что содержание файла зоны не было искажено при передаче.

В случае аварии или атаки необходим надежный контакт со

Таблица 3 Показатели уровня предоставления сервиса DNS по программе new gTLD

Показатель	Значение показателя (за месяц)
Доступность сервиса DNS	100%
Доступность сервера DNS	99%
Время отклика TCP DNS	1500 мс, для как минимум 95% запросов
Время отклика UDP DNS	500 мс, для как минимум 95% запросов
Время обновления зоны на DNS-узлах	60 минут, для как минимум 95% запросов

Рис. 2. Anycast облака зоны .ru.



службами эксплуатации на местах. Обычно это службы провайдера. Они должны вовремя отреагировать на атаку и просьбы о проведении каких-либо мероприятий. Отсутствие такого плотного взаимодействия во время атаки на турецкий национальный домен .tr было одной из причин его длительной (с 13 ноября по 27 декабря 2015 года)[21] неработоспособности.

Еще один важный момент, который связан с внедрением anycast на DNS-узлах, это установление и поддержание определенного уровня сервиса (соблюдение SLA). Наиболее известный в настоящее время такой документ – это приложение 10 к контракту на администрирование доменов верхнего уровня по программе new gTLD[22] (таблица 3).

В принципе, добиться таких показателей можно и без anycast при условии отсутствия атак. Но вот в условиях современного токсичного Интернета обеспечить их без технологии-anycast будет крайне сложно. Кроме того, время отклика DNS по UDP в 500 мс – это очень много. Примерно 25% пользователей веба прекращает загрузку страницы, если время ожидания загрузки превышает 4 секунды[23]. А на одной странице в настоящее время размещено несколько единиц контента, которые могут потребовать нескольких обращений к системе DNS.

Вообще говоря, SLA меняет сам принцип перераспределения трафика в DNS-сети, построенной по принципу anycast-облака. Главной целью построения сети становится не минимизация времени ответа резолверу, а максимизация количества обрабатываемых запросов в единицу времени при соблюдении условий SLA.

И в завершение раздела совсем чуть-чуть коснемся понятия «инцидент». Согласно ГОСТ Р 53114-2008[24], инцидентом информационной безопасности считается «любое событие, которое может нарушить деятельность или информационную безопасность». Нарушение информационной безопасности оставим в стороне и остановимся только на снижении уровня обслуживания. Деградация сервиса ниже уровня, определенного в SLA, не является в общем случае нарушением деятельности. Поэтому должен быть определен уровень предоставления сервиса, ниже которого ситуация будет определяться как «инцидент», и для этого случая необходимо прописать порядок действий. Соответствующие параметры должны быть указаны как для всей системы в целом, так и для «букв», отдельных узлов, серверов, а также каналов сервиса и управления.

Суха теория, мой друг...

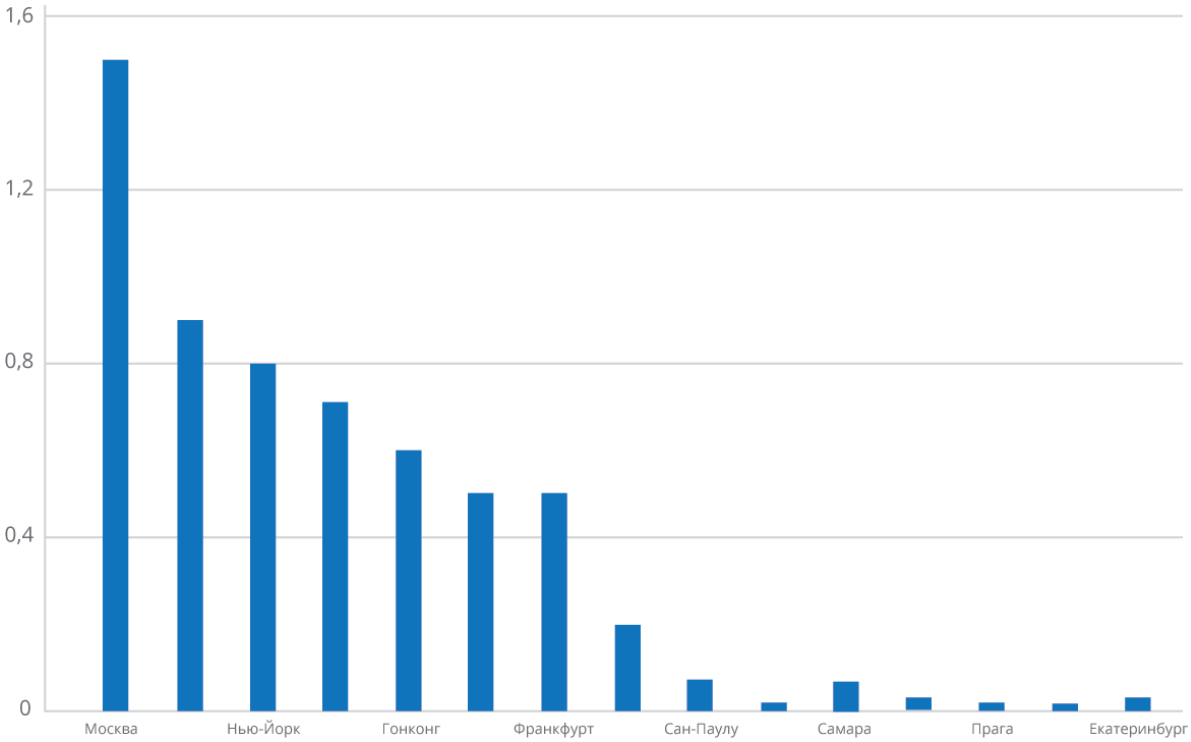
Теперь мы снова вернемся к примеру организации anycast-DNS-сети домена .ru. Домен поддерживает пять anycast-облаков. Отдельное облако для каждого географического региона показано на рисунке 2.

Таким образом, домен .ru поддерживает 35 авторитетных серверов, сгруппированных в 20 узлов, распределенных по пяти anycast-облакам.

Из названия облаков понятно, что используется принцип построения anycast-облаков по географическому признаку, т.е. geocast.

В среднем на всю систему при стационарных условиях (в отсутствие атак) приходится 5-6 миллиардов запросов в

Рис. 3. Нагрузка (млрд запросов/сутки).



сутки. В ситуации DGA-атаки система способна обрабатывать 8-9 миллиардов запросов в сутки.

По узлам в среднем при стационарных условиях наблюдаются показатели представленные на рисунке 3.

При размещении узлов системы DNS применяются следующие общие принципы:

1. Вынесение узлов в географически разнесенные локации (максимально приближенные к наиболее активным пользователям, применяется для глобальных узлов).
2. Максимальная концентрация локальных российских провайдеров в точке размещения узла (применяется для узлов на территории РФ).
3. Наличие свободных емкостей и удобство взаимодействия с площадкой (применяется для локальных узлов).
4. Размещение узлов в сетях провайдеров, которые могут обеспечить защиту от DDoS-атак, «очистку» трафика на своих каналах.

Максимальное приближение узлов к сетям конечных пользователей предполагает размещение узла либо на узлах Internet eXchange (IX), либо в сетях национальных провайдеров, например, «Ростелекома», либо в сетях глобальных провайдеров, например, LEVEL3.

Размещение на узлах IX позволяет организовать обмен трафиком с большим количеством региональных провайдеров «последней мили».

Сети национальных провайдеров, как правило, используются в качестве транзитных региональными провайдерами, что также позволяет приблизиться к большому количеству конечных клиентов.

Сети глобальных провайдеров позволяют встать на «трубе», по которой ходит мировой интернет-трафик. На своей «трубе» только сами эти провайдеры могут обеспечить защиту от DDoS-атак, т.к. необходимые решения для такой пропускной способности чрезвычайно дороги.

Подводя черту...

Тема реализации сервиса DNS на основе технологии anycast обширна. Охватить все аспекты и нюансы в одном материале невозможно. Остались за бортом вопросы организации сети резолверов на anycast-адресах, реализация DNS в сетях CDN и многое другое.

Технология anycast позволяет решить многие проблемы и задачи DNS. Но она также порождает новые задачи и проблемы.

Реализация DNS-облаков требует глубокого анализа DNS-статистики, продуманных инженерных решений и высокой квалификации обслуживающего персонала.

Тем не менее, на данный момент anycast – это наиболее стабильное и надежное решение для построения высоконагруженных DNS-сервисов, к которым предъявляются высокие требования по устойчивости и надежности.

Ссылки

1. В Орегоне и Франкфурте в сети Amazon нет серверов, поддерживающих домен .ru, но там в AWS установлены на виртуальных машинах серверы доменных имен, которые можно опросить.

2. https://tools.ietf.org/html/rfc5001

3. https://tools.ietf.org/html/rfc1546

4. https://www.ietf.org/rfc/rfc3258.txt

5. https://tools.ietf.org/html/rfc1997; https://tools.ietf.org/html/rfc3765

6. http://c.root-servers.org/october21.txt

7. Для обозначения имен серверов, поддерживающих корень системы DNS, принята нотация типа A.ROOT-SERVERS.NET. Более подробно смотри http://root-servers.org/

8. https://www.sans.org/reading-room/whitepapers/dns/secure-root-dns-servers-991

9. https://www.icann.org/en/system/files/files/factsheet-dns-attack-08mar07-en.pdf

10. https://www.rfc-editor.org/rfc/dfrfc/rfc1546.txt.pdf

11. https://tools.ietf.org/html/rfc3258

12. http://www.root-servers.org/news/events-of-20151130.txt

13. https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

14. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

15. https://blog.radware.com/security/2016/11/insight-into-mirais-source-code/

16. https://threatpost.com/dns-based-amplification-attacks-key-on-home-routers/105220/

17. https://www.isc.org/downloads/bind/

18. https://www.nlnetlabs.nl/projects/nsd/

19. https://atlas.ripe.net/

20. https://tools.ietf.org/html/rfc1034#section-4.3.5; https://tools.ietf.org/html/rfc5936

21. http://hello.nexusguard.com/hubfs/Threat_Report_Q4_2015_1.25.16.pdf?t=1456951275492

22. https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf

23. https://blog.kissmetrics.com/loading-time/

24. http://tdocs.su/22073

«Стильно, модно, молодежно...», или DNS & Blockchain

Павел Храмцов

Если не углубляться в криптографические подробности, то технология Blockchain позволяет вести распределенный реестр всего, чего угодно. И раз в системе DNS есть реестры, то было бы грех не попробовать реализовать их на этой новой технологии. Итак, мы имеем как минимум двух претендентов на реализацию: реестр доменов верхнего уровня и реестр изменений файла зоны. В настоящее время известны несколько реализаций реестров доменов на технологии Blockchain. Наиболее «старая» версия такой реализации – это проект NameCoin. Считается, что NameCoin – это одно из первых ответвлений от Bitcoin. Другой альтернативой традиционной системе DNS на основе технологии Blockchain является система ENS (Ethereum Name Service), построенная на основе smart-контрактов системы Ethereum.

В качестве вступления: у истоков, или «от печки»

Краеугольным камнем в основании корпорации ICANN является так называемый Белый документ (White Paper)[1]. Он был частью большой программы администрации президента Клинтона по построению Глобальной системы электронной коммерции (Clinton Administration's Framework for Global Electronic Commerce)[2].

Суть документа состоит в том, чтобы изменить существовавший на тот момент времени порядок распределения инфраструктурных информационных ресурсов (доменные имена и адреса), а именно превратить этот процесс в легитимный бизнес на основе свободной и честной конкуренции частных компаний.

Управление адресным пространством мы оставим за скобками, тем более что, согласно документу, их (адресов) распределение следовало отделить от управления пространством имен.

Весь технологический процесс регистрации доменов был разбит на три бизнес-составляющих: бизнес регистратуры, бизнес реестра и бизнес регистратора.

Регистратуры должны были быть независимыми некоммерческими организациями, которые определяют правила регистрации.

Реестры должны осуществлять функции ведения реестра доменных имен второго уровня, которые регистрируются в качестве поддоменов в доменных именах верхнего (первого) уровня.

Регистраторы должны осуществлять связь между администратором (владельцем) домена и реестром, т.е. выполнять операции регистрации нового домена, продлевать регистрацию домена и выполнять другие сервисные функции, которые могут привести к повышению качества обслуживания клиентов – администраторов доменов.

Отдельно были оговорены функции и сервис, читай бизнес, по поддержке собственно DNS, в части управления серверами доменных имен корня системы DNS.

На основе данного документа в 1998 году была создана ICANN и система распределенной регистрации. Однако распределенная система управления реестром так и не была создана до сих пор.

А о возможности такой системы управления реестрами в 1996 году в своем драфте[3] писал Джон Постел. Он задался вопросом: «Есть ли практический способ разделить единственное доменное имя между конкурирующими реестрами?» И ответил, что, возможно, есть техническое решение этой проблемы. Однако в том, что есть административное решение данной проблемы, он уверен не был. В итоге было принято решение, что у конкретного домена верхнего уровня регистратура может быть только одна, а вот регистраторов может быть сколь угодно много.

Конкуренция между регистратурами может существовать только в рамках конкуренции разных доменов, что открыло путь к появлению новых доменов верхнего уровня.

И вот сегодня, на пике популярности технологии Blockchain, мы имеем возможность построить распределенную регистратуру и обеспечить функционирование системы DNS на основе этой новой технологии. Клиент, конечно, не может переносить домен из регистратуры в регистратуру. Но единообразное качество услуги ему будет гарантировано самой технологией.

Но прежде чем перейти к описанию примеров, рассмотрим некоторые технологические особенности традиционной DNS.

И снова, в который раз: как устроена система DNS

Довольно часто при рассмотрении принципов функционирования DNS как бизнес-процесса смешивают в «одну посуду» несколько совершенно различных технологических процессов. А их как минимум три: управление реестром имен, делегирование прав управления доменами и поддержка DNS-инфраструктуры (серверов).

Реестр

Регистрация прав на управление доменом в реестре непосредственно к самой системе DNS как к технологическому процессу трансляции имени отношения не имеет. Регистраторы с реестром взаимодействуют по протоколу EPP[4]. В рамках этого взаимодействия в базе данных реестра создается множество объектов, например:

Domain – описывает доменное имя и параметры его регистрации;
Host – описывает серверы доменных имен, которые поддерживают домены;
Contact – описывает данные администратора домена;
Registrar – описывает параметры регистратора.

Делегирование

Связь с процессом трансляции имени у реестра появляется тогда, когда реестр генерирует и выгружает на DNS-сервер файл зоны, где каждому домену поставлены в соответствие серверы доменных имен, которые обслуживают домены.

На первый взгляд «оторванность» реестра от собственно самой распределенной системы DNS (множества серверов доменных имен) не должна приводить к каким-либо проблемам, но это не так. Например, до сих пор существует так и не урегулированный вопрос «orphan glue records», которому при запуске программы new gTLD[5] были посвящены отдельные рекомендации комитета советников по вопросам безопасности и стабильности (SSAC)[6].

В случае, когда обслуживание зоны производится на серверах с именами в той же зоне, для трансляции имени в родительской зоне необходимо явно указать IP-адрес этого сервера. В противном случае, получается циклическая зависимость – для доступа к зоне необходим доступ к серверу, на который делегирована зона, а для этого необходима трансляция его имени, для которой необходим доступ к зоне. Например, домен example.com делегирован на серверах ns1.example.com и ns2.example.com. В зоне example.com необходимо явно указать их IP-адреса. Эта запись называется «склеивающей» - «glue record».

При снятии или изменении делегирования с «glue record» могут возникнуть проблемы. Дело в том, что, например, информация о снятии делегирования с домена не может

быть автоматически распространена на управление объектом типа Host (сервер доменных имен) даже в рамках реестра. И тем более изменение информации на серверах доменных имен не может автоматически повлиять на содержание реестра. Например, изменение соответствия между доменным именем и IP-адресом сервера доменных имен в системе DNS должна быть «пронесена» регистратором отдельной командой EPP в реестр.

Другими словами, если в файле зоны example.com поменялось соответствие между именем ns2.example.com и IP-адресом, то для того, чтобы данное изменение было корректно отображено в реестре, объект Host, который соответствует ns2.example.com, должен быть также изменен – должен быть прописан новый IP-адрес. Иначе в зону в качестве glue-record попадет старое значение IP-адреса и система DNS будет работать некорректно.

Делегирование права на управление доменом в системе DNS реализуется путем прописывания серверов доменных имен для этого домена в файле зоны домена верхнего уровня администратором этого домена (домена верхнего уровня).

Для доменов верхнего уровня это делает IANA (PTI) в так называемой корневой зоне (root zone), для доменов второго уровня это делают реестры, а вот для доменов следующих в иерархии имен уровней это делают администраторы доменов верхнего уровня без процедуры автоматической генерации файла зоны из реестра.

Каждый раз, когда в файл зоны вносятся изменения, у него меняется серийный номер. При желании все множество версий файла зоны можно рассматривать в качестве реестра изменений. Вероятность того, что серийный номер повторится, чрезвычайно мала.

Инфраструктура

И последнее – это протокол DNS, который реализован на серверах доменных имен и резолверах. Он помогает использовать систему DNS в качестве большой поисковой машины. При этом машины универсальной. Дерево доменов позволяет быстро, и это ключевое свойство системы, искать как IP-адреса по заданным именам, так и имена по заданным адресам.

Некоторое время назад, до внедрения DNSSEC, оставались вопросы по достоверности информации, которую может получить пользователь из системы DNS. Внедрение DNSSEC эти вопросы снимает.

Тем не менее, один принципиально важный вопрос до сих пор не решен – это вопрос децентрализации управления пространством имен.

В корневой зоне изначально такое управление осуществляли госорганы США, потом управление было передано ICANN – частной некоммерческой корпорации.

Теперь, в эпоху бурного развития технологий Blockchain, многие из ее энтузиастов считают, что настало время перейти к полностью децентрализованной модели, когда единого центра управления не будет совсем.

В поиске альтернатив: DNS & Blockchain

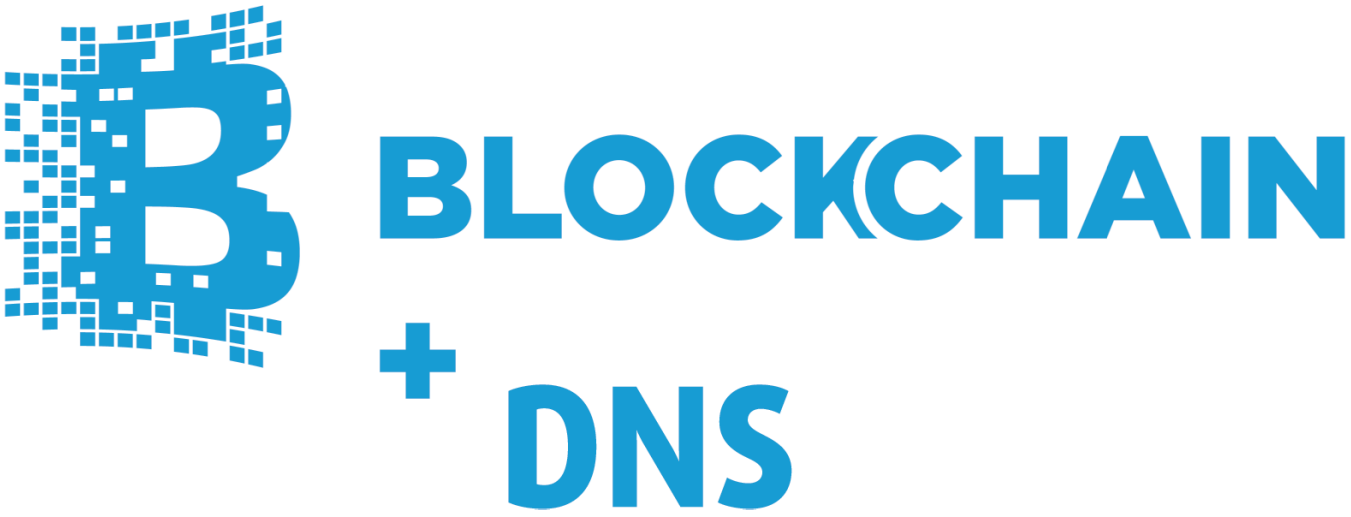
Если не углубляться в криптографические подробности, то технология Blockchain позволяет вести распределенный реестр всего, чего угодно. И раз в системе DNS есть реестры, то было бы грех не попробовать реализовать их на этой новой технологии.

Итак, мы имеем как минимум двух претендентов на реализацию: реестр доменов верхнего уровня и реестр изменений файла зоны.

В настоящее время известны несколько реализаций реестров доменов на технологии Blockchain.

Наиболее «старая» версия такой реализации – это проект NameCoin, который стартовал в 2010 году. Считается, что NameCoin – это одно из первых ответвлений от Bitcoin.

Мотивация создателей NameCoin проста – создать децентрализованную, защищенную от цензуры и вмеша-



тельства извне систему доменных имен, альтернативную существующей. Оставив политические аспекты типа SOPA[7] за скобками обсуждения, обратим все внимание на технологические аспекты.

Авторы проекта утверждают[8], что для реализации реестра и системы DNS не нужны DNSSEC и прочие ухищрения. Достоверность информации, в нашем случае - принадлежность имени администратору и соответствие имени конкретному адресу, обеспечивается самой технологией Blockchain.

Приватность информации, в данном случае речь идет о содержании DNS-запросов, достигается либо установкой копии реестра на компьютере конечного пользователя, либо за счет шифрования запросов при использовании DNSCurve при обращении к системе со стандартного резолвера.

Утверждается также, что NameCoin отвечает на запросы конечных клиентов быстрее, чем традиционная система DNS. Обоснование здесь такое – вся система находится на компьютере конечного клиента и время доступа в этом случае будет ~10 ms, в то время как в традиционной системе среднее время отклика - 100 ms.

В работе также приводятся соображения, что регистрация, обновление статуса домена и обновление информации в зоне будут также происходить быстрее. Для подтверждения регистрации, обновления и делегирования требуется подтверждение 12 последующих блоков в цепочке блоков. На майнинг одного блока уходит примерно 10 минут, т.е. на регистрацию домена потребуется примерно два часа, впрочем, как и на любую другую операцию.

Если резюмировать принцип работы NameCoin, то реестр и система резолвинга устанавливаются на компьютерах конечных пользователей. Реестр регистрации доменов (соответствие имени администратору) ведется по технологии Blockchain и реестр соответствия имен адресам (аналог зонных файлов) также ведется по технологии Blockchain.

Многие из описанных преимуществ NameCoin перед традиционной DNS выглядят с технической точки зрения и с точки зрения современных реализаций традиционной DNS неубедительно.

Во-первых, ничего не говорится о времени синхронизации реестров на компьютерах конечных пользователей.

Во-вторых, два часа на регистрацию имени – это по современным меркам очень много. Например, для системы регистрации освобождающихся доменов такие временные интервалы - в силу особенности бизнес-процесса - просто неприемлемы.

В настоящее время известны несколько реализаций реестров доменов на технологии Blockchain:

Наиболее «старая» версия такой реализации – это проект **NameCoin**, который стартовал в 2010 году. Считается, что NameCoin – это одно из первых ответвлений от Bitcoin.

Другой альтернативой традиционной системе DNS на основе технологии Blockchain является **система ENS (Ethereum Name Service)**, построенная на основе smart-контрактов системы Ethereum.

В-третьих, основное время сейчас тратится на подписание больших зон в рамках технологии DNSSEC, а не на их распространение. Для примера, в SLA по программе new gTLD время от внесения изменения в зону по протоколу EPP до появления изменения на серверах равно 60 минутам. Это в два раза меньше времени подтверждения в NameCoin при, например, делегировании домена. В реальной жизни такие изменения вносятся еще быстрее, в течение 10-15 минут, а то и быстрее.

Как бы то ни было, каждый желающий может попробовать систему в действии[9]. С ней ассоциирован домен верхнего уровня .bit. Это неофициальный домен верхнего уровня, «освященный» ICANN, но вполне работоспособный в рамках самой системы NameCoin.

Другой альтернативой традиционной системе DNS на основе технологии Blockchain является система ENS (Ethereum Name Service)[10], построенная на основе smart-контрактов системы Ethereum.

Система технологически состоит из двух типов компонентов: реестра и резолвера.

Реестр содержит информацию для всех доменов и поддоменов об администраторе домена, резолвере домена и времени жизни всех ресурсных записей, которые связаны с доменом.

Главное назначение резолвера – обеспечивать поиск соответствия между именем и адресом. При этом в документации оговаривается, что поиск соответствия предполагает нечастое обновление этого самого соответствия.

Регистратор в системе ENS - это smart-контракт, который регистрирует домены в соответствии со спецификацией EIP 162[11]. В случае, когда на регистрацию одного и того

же имени претендует несколько клиентов, включается аукцион доменов. Длительность типового аукциона пять дней. Платят за регистрацию Эфиром (монета Ethereum).

Таким образом, можно констатировать, что и здесь мы имеем дело с реализацией в технологии Blockchain как реестра имен, так и реестра файла зон.

Существуют и другие примеры построения альтернативной системы DNS на основе технологии Blockchain со шлюзами в обычный DNS. Например, EmerDNS[12] (EmcDNS) на основе Emercoin. Возможно, что эта система наиболее продвинута в сторону обычных пользователей. Для нее существуют плагины для браузеров, шлюз в альтернативные DNS и ряд других инструментов интеграции ресурсов системы с традиционным DNS.

Вместо заключения: в поиске «места под солнцем»

Практически все энтузиасты Blockchain фокусируют внимание на том, что технология позволяет построить полностью децентрализованный реестр, обеспечивает безопасность функционирования и защиту приватной информации.

При этом они опускают реализацию половины бизнес-процессов, которые сейчас доминируют в системе DNS, например, поддержку обратных зон или управление теми же orphan glue records.

Возможно, что таких проблем в новой системе может и не возникнуть, однако никто даже не начал обсуждать такие задачи, а дьявол, как известно, кроется в деталях.

Создание 20 лет назад корпорации ICANN было обосновано необходимостью и возможностью построения новых бизнес-моделей и бизнес-ролей: регистратура, регистратор, тр. В современных Blockchain-реализациях альтернативной DNS эти или новые роли четко не определены.

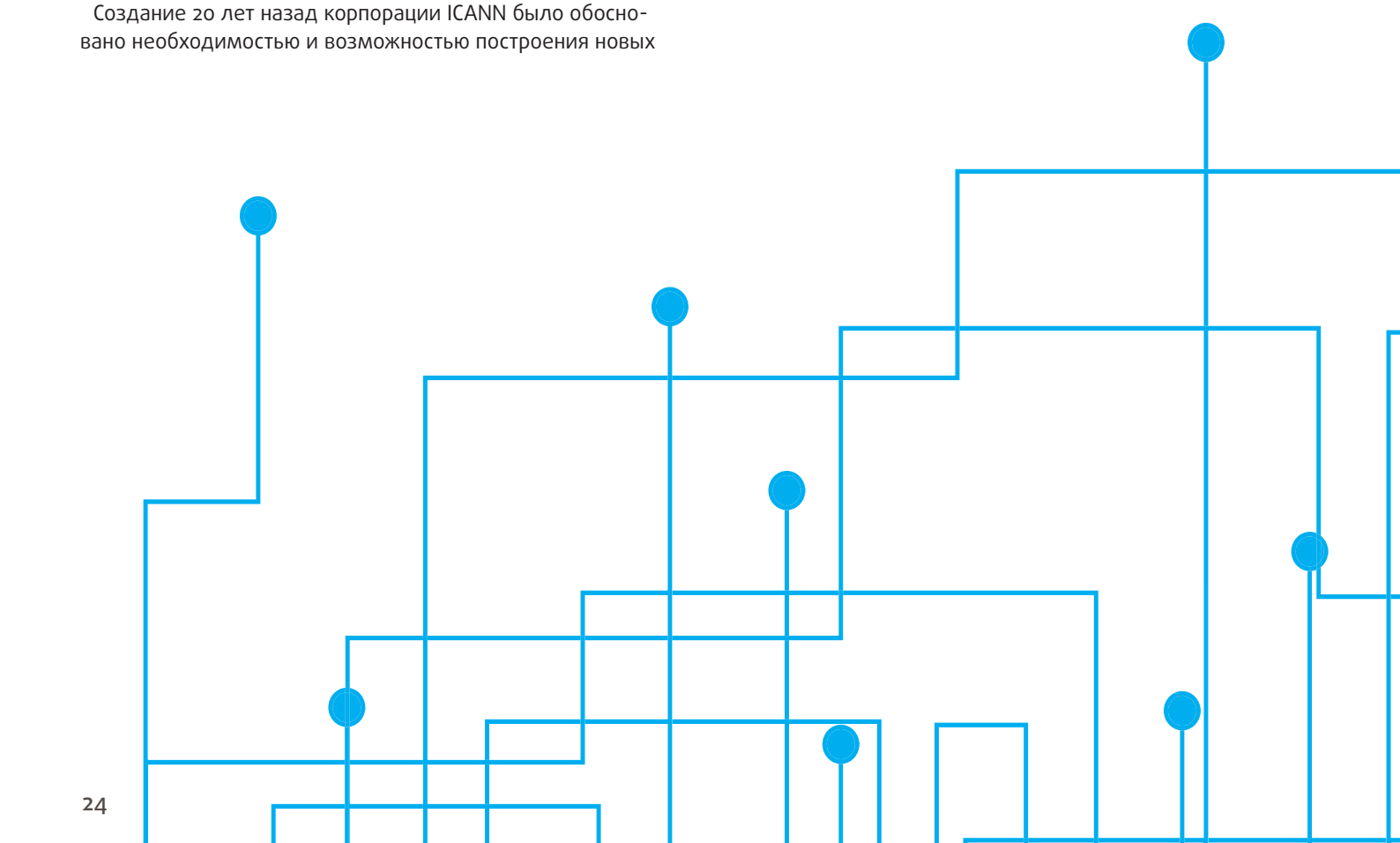
Есть майнеры, которые подтверждают транзакции. Они получают вознаграждение за свою работу. Есть разработчики приложений (smart-контрактов, например), которые тоже получают вознаграждение. Оплате подлежит подтверждение каждой транзакции: регистрация домена, смена IP-адреса сервера и т.п.

Ценообразование динамическое. Если, например, взять Ethereum, то нужно понимать, сколько «газа» нужно для конкретной операции и сколько стоит каждый «галлон». Для конечного пользователя может оказаться сюрпризом необходимость оплаты смены IP-адреса веб-сайта. В текущих реалиях это делается совершенно бесплатно через интерфейс регистратора/хостинг-провайдера.

Довольно часто звучит тезис о том, что технология Blockchain может «похоронить» ICANN, лишив корпорацию ее доминирующей роли в управлении пространством доменных имен. В этой связи хочется заметить, что упоминание технологии Blockchain в панельных дискуссиях на конференциях ICANN отмечено с 2015 года[13].

Следует также отметить, что проект NameCoin был представлен на 58-ой конференции ICANN в Копенгагене в 2017 году. Он вызвал довольно оживленную дискуссию и был воспринят сообществом положительно.

Принять на эксплуатацию 332 миллиона доменных имен не так-то просто. А пока NameCoin, например, осваивает пространство TOR (домен .onion)[14].



Ссылки

1. https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en#N_3_

2. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

3. http://userpage.fu-berlin.de/~mr94/dns/stuff/draft-postel-iana-itld-admin-01.txt

4. https://tools.ietf.org/html/rfc5730

5. https://newgtlds.icann.org/en/

6. https://www.icann.org/en/system/files/files/sac-048-en.pdf

7. https://ru.scribd.com/document/70419349/E-PARASITES-Act

8. https://www.sidnlabs.nl/downloads/theses/Report%20Namecoin%20as%20alternative%20to%20the%20Domain%20Name%20System.pdf

9. https://namecoin.org/

10. https://ens.domains/

11. https://github.com/ethereum/EIPs/issues/162

12. https://emercoin.com/en/tech-solutions/3#services

13. https://www.icann.org/en/system/files/files/iti-report-15may14-en.pdf

14. https://www.namecoin.org/files/videos/icann-58/Namecoin-ICANN58-TEG-Final.pdf

Защищенный DNS

Андрей Робачевский

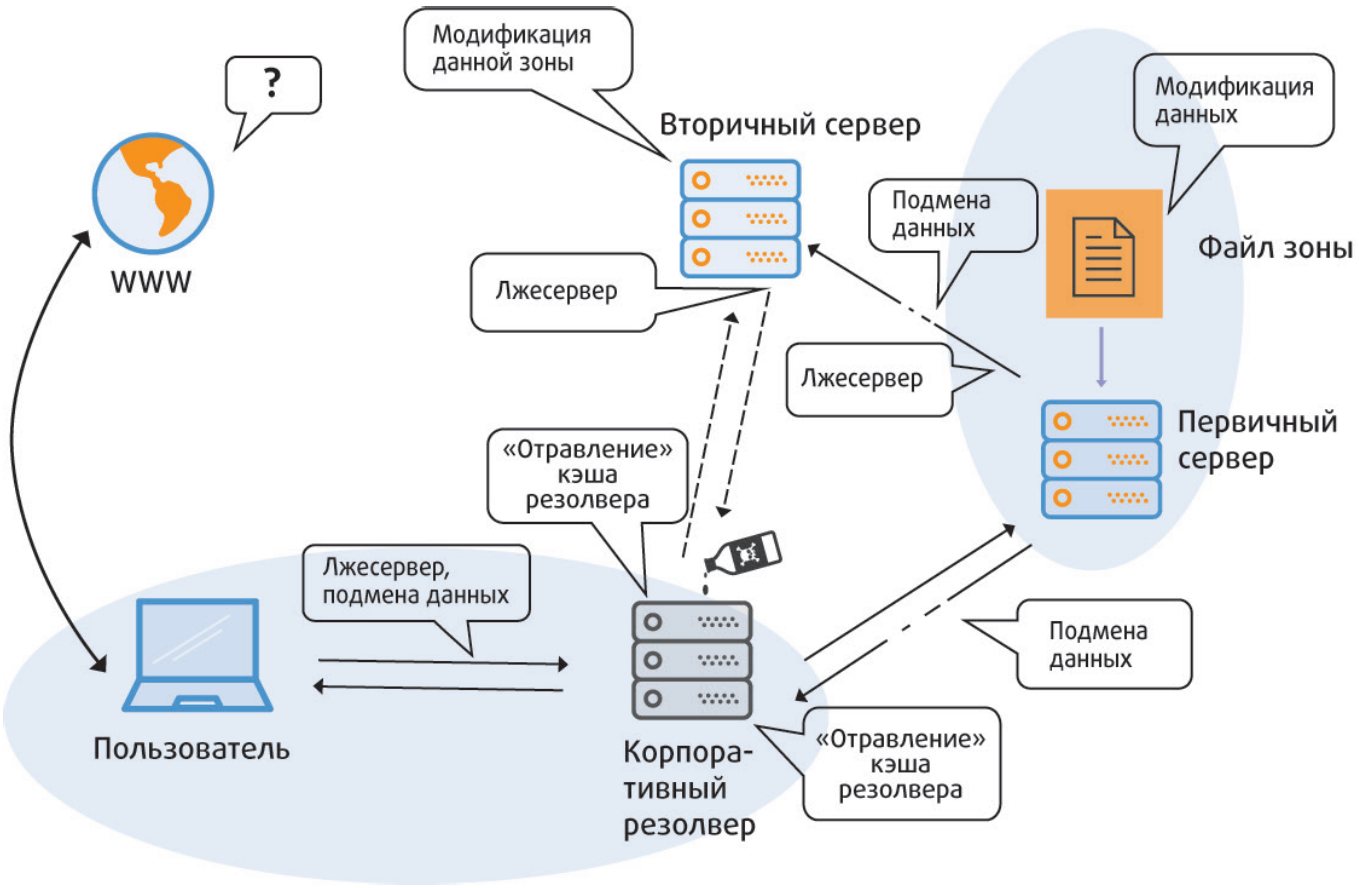
В рамках IETF были расширены возможности стандартного протокола DNS для решения проблемы аутентичности и целостности данных. Эти расширения получили название DNSSEC. При широкомасштабном внедрении технология DNSSEC позволяет эффективно решить проблему модификации данных, тем самым существенно увеличивая степень безопасности и доверия в Сети.

Внедрение DNSSEC также открывает новые возможности широкому применению и распространению других технологий безопасности, таких как DANE, и как следствие, уменьшает число случаев спама и подложных веб-сайтов.

Почти каждое обращение к информационным ресурсам Интернета начинается со взаимодействия с доменной системой имен DNS. Будь то посещение веб-сайта, обмен почтовыми сообщениями или общение в социальной сети, для определения фактического нахождения ресурса, а именно его IP-адреса, необходима DNS. Эта система обеспечивает трансляцию имени ресурса (например, facebook.com) в его IP-адрес (2a03:2880:f129:83:face:booc::25de), необходимый для установления связи.

Система DNS является иерархической и распределенной. Каждый из компонентов доменного имени обслуживается независимым оператором, а трансляция имени происходит посредством последовательного обращения к серверам, обслуживающим базы данных этих имен, или «зон», за ответом. Ответом может быть или указание на сервер, обслуживающий следующий компонент имени (т.н. реферрал), или окончательный ответ.

Рис. 1. Уязвимые места DNS.



К сожалению, этот процесс уязвим для различного рода атак. Причиной является слабая система защиты данных базового протокола DNS. Это означает, что в процессе передачи данных от сервера к клиенту данные могут быть модифицированы. Также возможно создание ложных DNS-серверов, поставляющих модифицированные данные. Последствия могут быть долгосрочными и значительными, как для отдельной группы пользователей, так и для отдельного сегмента сети Интернет.

Для того чтобы лучше понять важность обеспечения безопасности DNS, рассмотрим, насколько уязвима система в целом. Различные уязвимые места системы показаны на рисунке 1, а методы защиты - на рисунке 2.

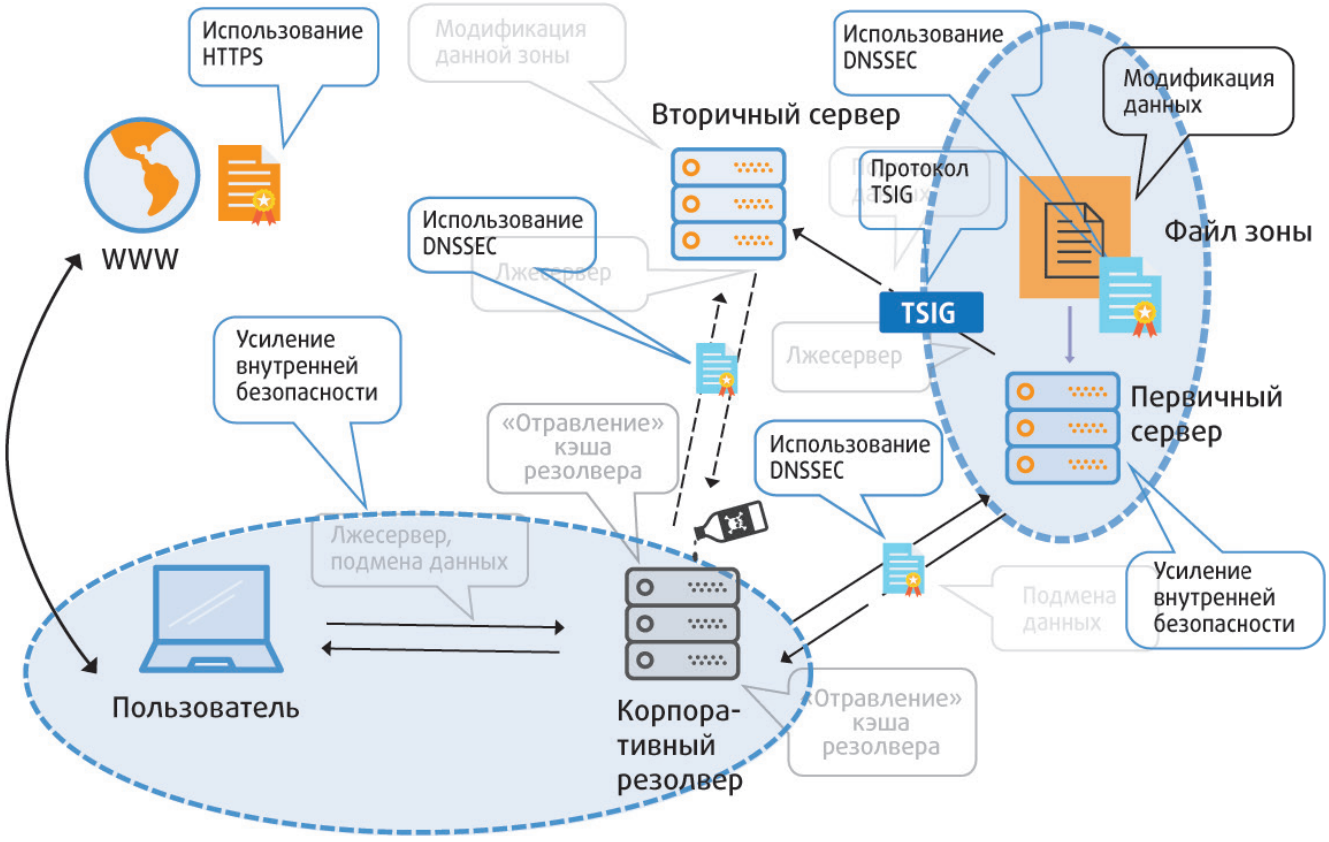
Первый вопрос - насколько защищен собственно процесс подготовки данных, редактирования и создания зоны DNS. Ошибочные данные, умышленно или случайно оказавшиеся в зоне, например, неправильные адреса веб-сайта или почтовых серверов, будут переданы пользователю в ответ на его запрос независимо от использования протоколов защиты DNS, таких как DNSSEC. В данном случае значение имеет уровень внутренней безопасности и защищенности процесса.

Данные также могут быть модифицированы при передаче от мастер-сервера ко вторичным DNS-серверам, обслуживающим зону. Сегодня для проверки целостности передачи данных используется протокол TSIG (Transaction SIGnature), описанный в стандарте IETF RFC 2845 «Secret Key Transaction Authentication for DNS (TSIG)» (https://datatracker.ietf.org/doc/rfc2845).

Ответы от DNS-серверов также могут быть модифицированы в процессе передачи в Интернете, но, пожалуй, наибольшую опасность представляет попадание неправильных данных в кэш итеративных резолверов - так называемое отравление кэша. Дело в том, что продолжительность жизни данных в кэше, определяемая параметром TTL записи ресурса (например, IP-адрес веб-сайта), может быть достаточно значительной. Это означает, что в течение всего этого времени при модификации данных кэша пользователи будут получать подложные ответы. Более того, внедрение подложных данных в кэш резолвера не представляет особого труда, как было продемонстрировано Дэном Камински в 2008 году (http://news.cnet.com/8301-1009_3-10009827-83.html). С тех пор в программное обеспечение большинства стандартных резолверов были введены изменения, усложняющие проведение атаки, но только DNSSEC является единственным эффективным методом защиты, поскольку позволяет криптографически проверить аутентичность данных перед загрузкой их в кэш.

Еще одной возможностью публикации ложных данных в DNS является создание лжесерверов DNS. Поскольку адресация и доступ к серверам происходит по их IP-адресу, атака на систему маршрутизации, а именно "захват" соответствующего адресного префикса, может привести к перенаправлению части запросов DNS к DNS-серверу злоумышленника. Соответственно, злоумышленник получает возможность публикации ложных данных с далеко идущими последствиями. Данная угроза особенно значительна при масштабном внедрении технологии аникаст, когда несколько серверов, расположенных в различных частях Интернета, используют один и тот же

Рис. 2. Методы защиты DNS.



IP-адрес. В этом случае отличить достоверный DNS-сервер от лжесервера становится сложнее.

Наконец, ответы резолвера на запросы клиентов могут быть также модифицированы. DNSSEC здесь не поможет, если пользователь не производит проверку подлинности ответов самостоятельно, а полагается на резолвер. Правда, канал между резолвером и пользователем как правило находится под административным контролем сервис-провайдера или администратора корпоративной сети, и зачастую имеет высокую степень защиты, например, с помощью VPN.

Эффективным средством противостояния последствиям модификации данных DNS является применение расширений безопасности DNS, разработанных в рамках IETF (Internet Engineering Task Force, www.ietf.org) и получивших название DNSSEC.

Как защитить DNS?

Давайте теперь поговорим более подробно о технологии, позволяющей защитить многие уязвимые места DNS, связанные с целостностью и аутентичностью данных.

В рамках IETF были расширены возможности стандартного протокола DNS для решения проблемы аутентичности и целостности данных. Эти расширения получили название DNSSEC. Основная спецификация DNSSEC содержится в стандартах IETF RFC4033 (https://datatracker.ietf.org/doc/rfc4033), RFC4034 (https://datatracker.ietf.org/doc/rfc4034), RFC4035 (https://datatracker.ietf.org/doc/rfc4035) и RFC5155 (https://datatracker.ietf.org/doc/rfc5155).

С помощью DNSSEC пользователь имеет возможность убедиться, что полученные данные не были модифицированы в процессе публикации и передачи. Другими словами, убедиться в том, что данные, содержащиеся в ответе на запрос DNS, в точности соответствуют данным в зоне для запрашиваемого доменного имени.

В рамках стандартного подхода к информационной безопасности рассматриваются три основных аспекта данных - их конфиденциальность, целостность и доступность. Целью технологии DNSSEC является защита целостности данных, а точнее, обеспечение возможности проверки целостности данных. Конфиденциальность не является требованием в DNS, а доступность обеспечивается путем усиления инфраструктуры - например, использования технологии аникаст. Кстати, при использовании аникаст вопросы аутентичности и целостности данных встают еще острее, увеличивая ценность DNSSEC.

DNSSEC основан на криптографии с использованием открытых ключей. Администратор зоны подписывает все записи зоны своей цифровой подписью. Там же администратор публикует и открытый ключ, соответствующий этой цифровой подписи. Таким образом, путем проверки подлинности цифровой подписи и ее принадлежности администратору зоны пользователь может убедиться в целостности и аутентичности полученных данных.

Подлинность открытого ключа удостоверяет администратор родительской зоны путем включения в зону т.н. записи DS, представляющей собой хэш открытого ключа дочерней зоны. Разумеется, эта запись заверена цифровой подписью администратора этой родительской зоны. Его же ключ удостоверяется администратором зоны верхнего уровня - и так далее, пока не будет достигнута так называемая точка доверия (trust anchor) - ключ, которому пользователь абсолютно доверяет. В DNSSEC таким ключом является ключ корневой зоны «.».

Таким образом, для проверки подлинности ответа на запрос DNS пользователю необходимо совершить целую цепочку проверок - от корневого ключа до ключа зоны, содержащей доменное имя. Этот процесс называется построением цепочки доверия. Только при успешном построении цепочки доверия и положительной проверке самой записи ответ может быть положительно удостоверен. Если хотя бы одна из проверок заканчивается неудачей, то и общий результат будет отрицательным.

К счастью, цепочка доверия DNSSEC полностью соответствует структуре делегирования имен, поэтому процесс построения цепочки доверия и разрешения имен происходит одновременно. На рисунке 3 показана цепочка доверия в DNSSEC.

Из рисунка, кстати, видно, что в DNSSEC используются два типа ключей – так называемый ключ KSK (Key Signing Key, ключ подписи ключей) и ключ ZSK (ключ подписи зоны). Первый является ключом долговременного пользования и, соответственно, более сильным в криптографическом плане. Именно хэш ключа KSK «экспортируется» в родительскую зону в виде записи DS, устанавливая тем самым цепочку доверия. Ключ ZSK служит для подписания записей самой зоны. Ключ ZSK удостоверяется администратором домена путем подписи его ключом KSK. Поскольку в изменении ZSK задействован только администратор домена, этот процесс может (и должен) происходить достаточно часто.

Еще одной важной особенностью DNSSEC является то, что он позволяет удостовериться, что запрошенное имя не существует. Другими словами, при запросе разрешения несуществующего имени пользователю будет возвращен криптографически заверенный ответ, указывающий на отсутствие запрашиваемой записи в зоне. Для этого в DNSSEC используются технологии NSEC и NSEC3 (http://ru.wikipedia.org/wiki/DNSSEC).

В то же время DNSSEC не является панацеей. Даже если полученные адреса серверов являются правильными, обмен данными может быть перехвачен или перенаправлен с использованием уязвимых мест системы маршрутизации. Также DNSSEC не обеспечивает шифрование данных, здесь необходима другая, довольно широко распространенная технология TLS (Transport Layer Security), использующая цифровые сертификаты X.509, на которой базируется протокол HTTPS. Наконец, DNSSEC не спасет от гомографии, когда имя сервера внешне очень похоже на другое имя, но на самом деле использует другие символы, например, «1» и «l».

И все же, использование DNSSEC совместно с другими средствами защиты существенно усиливает их эффективность. Например, в противоположность сертификатам доменных имен, используемых в TLS/HTTPS, цепь доверия в DNSSEC следует цепочке делегирования доменов и, таким образом, основана на деловых отношениях, существующих при регистрации доменов.

DANE

Внедрение DNSSEC также открывает новые возможности. Например, решить проблемы, связанные с сертификатами для проверки достоверности веб- или почтовых серверов и обмена информацией с использованием защищенного протокола TLS. Так называемая система Web-PKI.

Дело в том, что выдачей этих X.509-сертификатов занимаются несколько сотен независимых удостоверяющих центров (УЦ), которые используют данные третьих сторон (например, данные от компаний-регистраторов) для верификации прав пользования доменным именем. Конкретный список доверенных УЦ определяется производителями веб-браузеров – такими компаниями, как Google, Apple, Mozilla Foundation и т.д. Хотя в выборе УЦ они руководствуются требованиями CA/Browser Forum (https://cabforum.org/about-the-baseline-requirements/), а также результатами аудита WebTrust Task Force (http://www.webtrust.org/principles-and-criteria/item83172.aspx) и ETSI (https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx), в основном этот процесс закрыт и непрозрачен.

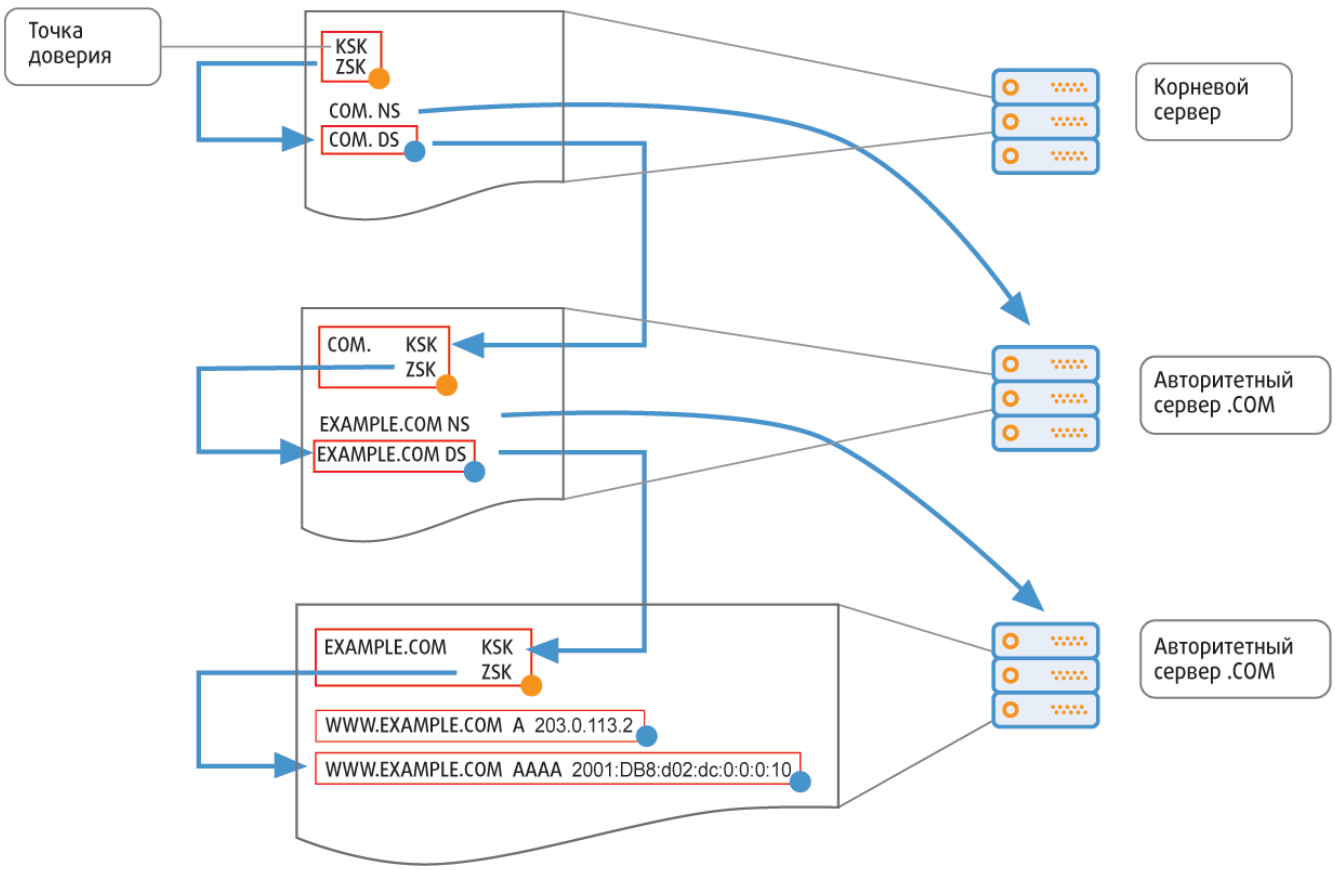
В Web-PKI все УЦ, корневые сертификаты которых установлены в браузере пользователя, имеют право выдавать сертификаты для любого доменного имени и при этом имеют одинаковый уровень доверия. Любой из этих корневых сертификатов является так называемой точкой доверия (trust anchor, TA). Это значит, что УЦ с недостаточным качеством проверок прав владения именем является «слабым звеном» всей системы. Злоумышленник может использовать такой УЦ для получения конкурирующего сертификата для уже существующего чужого имени или сертификата для несуществующего имени. Даже флагманы индустрии оказываются уязвимы – так, компания Symantec на протяжении нескольких лет генерировала сертификаты для несуществующих имен, с просроченным сроком действия и другими нарушениями требований CA/Browser Forum (https://wiki.mozilla.org/CA:Symantec_Issues).

Дело усугубляется еще и тем, что корневые УЦ часто делегируют полномочия выдачи сертификатов подчиненным УЦ. В результате в Интернете существует большое количество доверенных УЦ, качество регистрационных процессов которых проверить практически невозможно.

Исправить ситуацию можно, если владелец доменного имени сможет сам контролировать выдачу сертификатов, а по возможности – и вообще избежать услуг третьих лиц.

Здесь на помощь приходит DNS. Действительно, если владелец имени или зоны контролирует публикацию такой важной информации, как IP-адреса сайтов, почтовых серверов, обслуживающих домен, и т.п., почему бы не

Рис. 3. Построение цепочки доверия в DNSSEC.



создать новую запись, с помощью которой владелец смог бы указать на сертификат, который следует использовать при обращении к сайту, почтовому серверу и т.д.? Разумеется, эта запись должна быть защищена, и DNSSEC выполняет эту функцию.

Разработка и стандартизация соответствующих протоколов велась в рамках рабочей группы IETF DANE (http://datatracker.ietf.org/wg/dane/). DANE позволяет владельцу домена указать, какой сертификат TLS/SSL должно использовать приложение или служба для подключения к вашему сайту. Для этого используется запись TLSA, стандартизованная в RFC6698 "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA" (https://datatracker.ietf.org/doc/rfc6698) и RFC7671 «The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance" (https://datatracker.ietf.org/doc/rfc7671/).

Основой DANE является новая запись ресурса TLSA. Эта запись с доменным именем хоста и содержит инструкции по использованию TLS/SSL-сертификата при доступе к сервису по указанному порту и протоколу.

Так, например, следующая запись указывает, что необходимо использовать точку доверия (trust anchor, TA), указанную в последнем поле записи, при валидации сертификата, полученного при обращении к веб-серверу www.example.com по протоколу HTTPS (порт 443, протокол TCP):

```
_443._tcp.www.example.com.   IN TLSA 2 0 1 (
                             E8B54E0B4BAA815B06D3462D65FBC7C0
                             CF556ECCF9F5303EBFBB77D022F834C0 )
```

Поля после метки TLSA имеют следующее значение:

IN TLSA	2	0	1	E8B54E0B4BAA8…
	Использование сертификата	Селектор	Тип сравнения	Данные, ассоциированные с сертификатом
	0 – PKIX-TA 1 – PKIX-EE 2 – DANE-TA 3 – DANE-EE	0 – использовать весь сертификат для сравнения 1 – использовать только открытый ключ для сравнения	0 – все данные, указанные селектором, используются для сравнения 1 – хэш SHA-256 данных используются для сравнения 2 - хэш SHA-512 данных используются для сравнения	Данные, необходимые для сравнения, закодированные в виде строки BASE64

Давайте чуть подробнее остановимся на поле «Использование сертификата». Это поле определяет проверки, которые браузер с поддержкой DANE должен выполнить перед принятием решения об использовании сертификата, полученного от веб-сайта. Эти проверки схематично отображены на рис. 4.

Значение 0 (PKIX-TA) указывает, что путь валидации полученного сертификата, или открытого ключа, в зависимости от значения поля «Селектор», должен проходить через сертификат, указанный в поле «Данные, ассоциированные с сертификатом». Это может быть как корневой, так и подчиненный сертификат, но в любом случае путь валидации должен заканчиваться точкой доверия, зарегистрированной в пользовательском браузере.

Значение 1 (PKIX-EE) накладывает ограничение на сертификат, полученный от веб-сервера. Он (или его открытый ключ) должен соответствовать «данным, ассоциированным с сертификатом». При этом сертификат должен пройти проверку, используя путь валидации к одной из точек доверия браузера.

Значение 2 (DANE-TA) применяется для определения сертификата, который должен использоваться в качестве новой точки доверия при валидации сертификата, полученного от веб-сервера. Этот метод также называют «утверждением точки доверия», поскольку он позволяет владельцу доменного имени указать точку доверия, которая не входит в стандартную коллекцию TA пользовательского браузера.

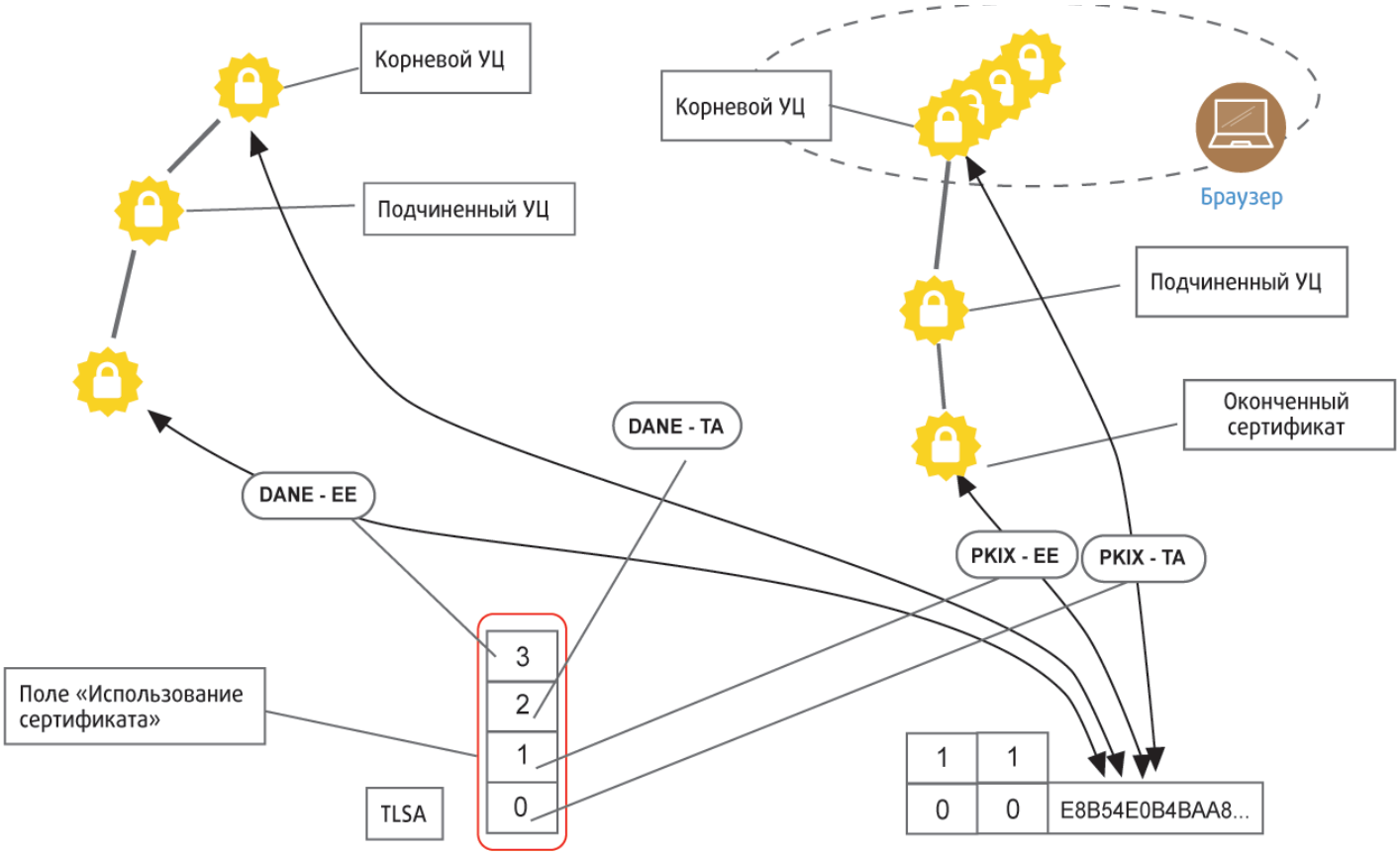
Наконец, **значение 3 (DANE-EE)** определяет метод, когда сертификат (или его открытый ключ), полученный от сервера, должен совпадать с сертификатом, указанным в записи TLSA. Этот метод позволяет владельцу доменного имени использовать собственные сертификаты без привлечения сторонних УЦ. Этот метод отличается от PKIX-EE тем, что не требует дополнительной валидации сертификата через путь доверия.

DANE может использоваться не только при взаимодействии с веб-серверами. Например, защита передачи данных между почтовыми серверами является чрезвычайно важной. При этом часто используется протокол TLS, но аутентичность сертификата сервера представляет еще большую проблему, чем в случае с Web-PKI. DANE и здесь окажет администраторам почтовых серверов неоценимую услугу, делая почтовую систему в целом более защищенной. Более подробно о проблематике защиты передачи почтовых сообщений между транспортными почтовыми агентами (Mail Transport Agent, MTA) и о применении DANE в этом случае для защиты протокола SMTP описано в RFC7672 "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)" (https://datatracker.ietf.org/doc/rfc7672).

Другие протоколы приложений, например, IMAP или XMPP, могут также использовать DANE. Обсуждение использования DANE в этих случаях можно найти в RFC 7673 "Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records" (https://datatracker.ietf.org/doc/rfc7673).

Другими словами, DNSSEC+DANE обладают существенным

Рис. 4. Различные типы записи TLSA и связанные с ними проверки.



потенциалом обеспечения защищенности коммуникационной инфраструктуры Интернета на уровне приложений. Основной проблемой является внедрение этих технологий. Дело в том, что их полноценное использование зависит от усилий многих сторон, интересы которых не обязательно совпадают. Так, например, даже если владелец доменного имени заинтересован в его защите с помощью DNSSEC и DANE, его успех зависит от многих факторов, находящихся вне его контроля:

- внедрен ли DNSSEC в родительской зоне?
- поддерживает ли регистратор доменов DNSSEC и DANE (включение в зону соответствующих записей, а также записи защищенного делегирования DS в родительской зоне)?
- выполняет ли резолвер пользователя валидацию DNSSEC?
- поддерживает ли пользовательское приложение (веб-браузер, почтовый сервер) протокол DANE?

Отрицательный ответ на хотя бы один из приведенных выше вопросов сведет на нет защиту, предоставляемую этими технологиями. Этим объясняются весьма невысокие цифры внедрения этих технологий: процент внедрения DNSSEC не превышает пары процентов (есть исключения – например, в Германии уровень внедрения достиг 12% (https://eggert.org/meter/dnssec)), а проникновение DANE (записей TLSA) в этих подписанных зонах и того меньше – он составляет всего 1,8%. Использование DNSSEC (валидация ответов) находится на уровне 15%, во многом благодаря широкому использованию открытого резолвера Google (Google Public DNS), который осуществляет валидацию ответов по умолчанию.

Однако не стоит отчаиваться. Знание этих возможностей - уже шаг в правильном направлении. Пользовательский интерес к защищенному DNS является существенным стимулом для внедрения сервис-провайдером DNSSEC и осуществления валидации запросов. Требования поддержки DNSSEC и DANE владельцев доменных имен будут рано или поздно услышаны регистраторами и операторами доменов.

Грядут большие перемены в основных протоколах Интернета

Марк Ноттинхем (Mark Nottingham)

Теперь основные протоколы Интернета претерпевают значительные изменения. На работу Интернета в общем и целом они не сильно повлияют (иначе бы их не приняли), но могут оказаться неприятным сюрпризом для тех, кто привык пользоваться недокументированными особенностями протоколов в неблаговидных целях... или просто привык рассчитывать на сохранение статус-кво. Когда протокол не может развиваться, потому что внедрение «заморозило» его точки развития, мы говорим, что он окостенел. Для предотвращения окостенения важно открыть протоколам возможность развиваться в соответствии с потребностями Интернета будущего; иначе случится т.н. трагедия общин, где действия некоторых сетей – пусть и лишенные злого умысла – могут подорвать «здоровье» всего Интернета.

Когда Интернет начал широко использоваться в 1990-х годах, большая часть трафика использовала всего несколько протоколов: IPv4 маршрутизировал пакеты, TCP превращал эти пакеты в соединения, SSL (а позднее TLS) эти соединения шифровал, DNS сообщал имена хостов для подключения, а протокол прикладного уровня HTTP все это использовал.

Шли годы, а эти протоколы – основные протоколы Интернета – изменились лишь в мелочах: в HTTP добавилось несколько новых заголовков и методов, TLS неспешно претерпел парочку мелких переработок, в TCP появился контроль перегрузки, а DNS обзавелся «фишечками» типа DNSSEC. Сами же протоколы в процессе передачи, как говорят – «на проводе» (on the wire), долгое время оставались практически теми же (за исключением IPv6, но эта тема и так получает достаточно внимания у сетевых операторов).

В результате сетевые операторы, поставщики услуг и законодатели, которые желают понять (а иногда и контролировать) Интернет, за долгие годы выработали ряд методов, основанных на «отпечатках» этих протоколов при передаче по каналу – и эти методы верно служат им для самых разных целей: будь то устранение неполадок, повышение качества обслуживания или навязывание политик.

Теперь же основные протоколы Интернета претерпевают значительные изменения. На работу Интернета в общем и целом они не сильно повлияют (иначе бы их не приняли), но могут оказаться неприятным сюрпризом для тех, кто привык пользоваться недокументированными особенностями протоколов в неблаговидных целях... или просто привык рассчитывать на сохранение статус-кво.

> Чтобы Интернет хорошо работал в долгосрочной перспективе, он должен приносить ценность конечным пользователям, не поддаваться окостенению и не мешать сетям работать.

Зачем нам нужно менять Интернет

Причин тому немало.

Во-первых, основные протоколы Интернета подошли к границам своих возможностей, в первую очередь в части быстродействия. Из-за структурных проблем в протоколах прикладного и транспортного уровней сеть используется неэффективно, в результате чего страдает конечный пользователь (в первую очередь мы говорим о задержке).

Это уже само по себе весомый аргумент в пользу доработки или замены устаревших протоколов, поскольку имеется множество свидетельств того, какой весомый эффект дает даже небольшое повышение быстродействия (https://www.smashingmagazine.com/2015/09/why-performance-matters-the-perception-of-time/).

Во-вторых, развивать и модифицировать протоколы Интернета – на любом уровне – со временем становится все труднее, в немалой степени из-за того, что (как уже говорилось) сети не всегда используют их строго по назначению. Например, HTTP-прокси, компрессирующие ответы, усложняют развертывание новых методов сжатия, а оптимизация TCP в сетевых приставках затрудняет внедрение доработанных вариантов TCP.

И, наконец, сейчас Интернет повсеместно внедряет шифрование (https://static.googleusercontent.com/media/research.google.com/en/pubs/archive/46197.pdf) после откровений Эдварда Сноудена в 2013 году. Эта тема вообще отдельная; но здесь нельзя не отметить, что шифрование – один из лучших имеющихся у нас инструментов, обеспечивающих протоколам возможность развиваться.

Теперь поговорим о том, что случилось, что будет дальше, как это может повлиять на сети и как сети влияют на дизайн протоколов.

HTTP/2

HTTP/2 (https://http2.github.io/) (выросший из Google SPDY) ознаменовал собой первую крупную реформу – ставший стандартом в 2015 году, этот протокол мультиплексирует запросы по одному соединению TCP, устраняя необходимость ставить запросы на клиенте в очередь, чтобы они не блокировали друг друга. Теперь этот протокол получил широкое распространение, поддерживается всеми основными браузерами и крупными веб-серверами.

С точки зрения сети, значительных изменений в HTTP/2 несколько. Во-первых, это двоичный протокол, т.е. любое устройство, которое примет его за HTTP/1.1, просто не будет работать.

В частности, поэтому в HTTP/2 введено еще одно крупное новшество: по сути, он требует шифрования. Дело в том, что при шифровании промежуточные устройства имеют меньше возможностей что-то напортить: либо обращаться с HTTP/2 как с HTTP/1.1, либо вносить менее заметные изменения, например, отрезать заголовки или блокировать новые расширения. Инженеры, участвовавшие в разработке нового протокола, столкнулись с обеими описанными ситуациями, и обе они вызвали значительные проблемы с поддержкой.

Кроме того, HTTP/2 требует использовать TLS/1.2 (и выше) для шифрования (http://httpwg.org/specs/rfc7540.html#TLSUsage), а также вносит в черный список (http://httpwg.org/specs/rfc7540.html#BadCipherSuites) шифронаборы, которые считает небезопасными — по сути, он допускает только эфемерные ключи. Вопрос о том, на что это может повлиять, мы обсудим в разделе, посвященном TLS 1.3.

И, наконец, HTTP/2 позволяет объединить несколько запросов хоста в одно соединение (http://httpwg.org/specs/rfc7540.html#reuse), повышая быстродействие за счет снижения числа подключений (а тем самым – и контекстов контроля перегрузки), необходимых для загрузки страницы.

Например, имеющееся подключение к www.example.com можно использовать для запросов к images.example.com. В будущих расширениях этого протокола, возможно, будет разрешено добавлять к соединению новые хосты (https://tools.ietf.org/html/draft-bishop-httpbis-http2-additional-certs), даже если они отсутствовали в исходном TLS-сертификате соединения. Получается, нельзя будет и дальше предполагать, что трафик по соединению ограничивается той целью, для которой это соединение было установлено.

Несмотря на перечисленные изменения, следует отметить, что HTTP/2 не обнаружил существенных проблем с совместимостью или помехами со стороны сетей.

TLS 1.3

TLS 1.3 (https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/) сейчас находится в финальной стадии стандартизации и уже поддерживается некоторыми реализациями.

Разработчики стандарта излишне поскромничали, назвав его TLS 1.3, а не 2.0: перед нами фактически новая версия TLS, с полностью переработанным рукопожатием, позволяющим передавать данные приложений с самого начала (это часто называют 0RTT). Новый протокол также полагается на обмен эфемерными ключами, не используя статических.

Это обстоятельство встревожило часть сетевых операторов и поставщиков – в первую очередь тех, кому требуется видеть, что происходит внутри соединения.

Например, центр данных крупного банка по закону должен обеспечивать прозрачность трафика. У него на серверах стоит сниффер, который анализирует трафик и дешифрует его с помощью статических ключей, чтобы регистрировать законный трафик и выявлять незаконный – и атаки извне, и попытки сотрудников организовать утечку данных вовне.

Такую методику перехвата трафика TLS 1.3 не поддерживает, потому что это еще и одна из форм сетевых атак, для защиты от которых и предназначены эфемерные ключи (https://en.wikipedia.org/wiki/Forward_secrecy). Но ведь тот же самый закон, который требует от банков осуществлять мониторинг своих сетей, предписывает им использовать современные протоколы шифрования. И как тут быть?

Было сломано много копий в спорах о том, действительно ли закон требует именно статических ключей, могут ли альтернативные подходы оказаться не менее эффективными – и стоит ли ради потребностей относительно немногих сетей поступиться безопасностью всего Интернета. И действительно, дешифровка трафика TLS 1.3 возможна, но для этого нужны эфемерные ключи, а они по самой своей сути долго не живут.

На сей момент непохоже, что разработчики TLS 1.3 модифицируют его так, чтобы учесть потребности таких сетей, но есть разговор о том, чтобы создать еще один протокол, который позволит третьей стороне наблюдать за происходящим – а возможно, и не только – специально для таких случаев. Время покажет, что из этого вырастет и вырастет ли.

QUIC

В процессе работы над HTTP/2 обнаружилось, что TCP страдает от той же самой неэффективности. Поскольку TCP – протокол с сохранением порядка пакетов, потеря одного может сорвать доставку всех последующих: они так и останутся в буфере. При мультиплексировании это может означать катастрофическую потерю быстродействия.

QUIC (https://quicwg.github.io/) – это попытка решить проблему, фактически воссоздав семантику TCP (вместе с частью потоковой модели HTTP/2) поверх UDP. Как и HTTP/2, QUIC первоначально разрабатывался Google, а теперь IETF развивает его, начиная с первоначального сценария использования «HTTP поверх UDP». Планируется сделать его стандартом к концу 2018 года. Однако поскольку Google уже внедрил QUIC в своем браузере Chrome и на своих сайтах, на него уже приходится более 7% интернет-трафика.

Помимо того, что столь значительный объем трафика перешел с TCP на UDP (т.е. сети должны адаптироваться к новой реальности), оба варианта QUIC – и Google QUIC (gQUIC), и IETF QUIC (iQUIC) – для работы требуют шифрования: незашифрованного QUIC не существует в принципе.

iQUIC использует TLS 1.3 для создания ключей сеанса, а потом шифрует ими каждый пакет. Но поскольку это надстройка над UDP, в QUIC шифруется множество того, что в TCP передается открыто – в частности, информация о сеансе и метаданные.

По сути, в нынешнем «коротком заголовке» (https://quicwg.github.io/base-drafts/draft-ietf-quic-transport.html#short-header) iQUIC, который используется для всех пакетов, кроме рукопожатия, открыты только номер пакета, необязательный идентификатор соединения и бит состояния, используемый для таких вещей, как график ротации ключей шифрования и тип пакета (причем они сами могут быть зашифрованы).

Все остальное зашифровано, включая ACK – очень интересный сюрприз для атак путем анализа трафика (https://www.mjkranch.com/docs/CODASPY17_Kranch_Reed_IdentifyingHTTPSNetflix.pdf).

С другой стороны, теперь невозможна пассивная оценка RTT и потери пакетов путем наблюдения за соединением, для этого не хватает информации. Поэтому некоторые сетевые операторы категорически против перехода на QUIC, они утверждают, что подобные пассивные измерения необходимы для отладки сетей и понимания их работы.

Уже появилось предложение, призванное решить эту проблему – так называемый бит-перевертыш (Spin Bit) (https://tools.ietf.org/html/draft-trammell-quic-spin): бит в заголовке, который переворачивается один раз при передаче в оба конца, чтобы наблюдатель смог аппроксимировать RTT. Поскольку этот бит никак не связан с состоянием приложения, он не выдает никакой информации о конечных точках соединения, кроме грубой оценки их расположения в сети.

DOH

Последнее из новых веяний на горизонте – это DOH, или DNS поверх HTTP (https://datatracker.ietf.org/wg/doh/about/). Исследования показали, что DNS в сетях регулярно используется в качестве средства навязывания политик (https://datatracker.ietf.org/meeting/99/materials/slides-99-maprg-fingerprint-based-detection-of-dns-hijacks-using-ripe-atlas/) (как от лица сетевого оператора, так и от лица властей).

Некоторое время обсуждалась идея обойти этот вид контроля с помощью шифрования (https://datatracker.ietf.org/wg/dprive/about/), но недостатком такого решения (по крайней мере, с некоторых точек зрения) является возможность выделить подобный трафик из общей массы – например, заблокировать его по номеру порта.

DOH решает эту проблему, «растворяя» трафик DNS в существующем соединении HTTP и тем самым просто убирая демаскирующие элементы. Теперь, чтобы заблокировать доступ к такому DNS-преобразователю, придется заблокировать и доступ к веб-сайту.

Например, если Google решит перевести на DOH свою общедоступную службу DNS (https://developers.google.com/speed/public-dns/) на www.google.com, а пользователь настроит свой браузер на работу с этой DNS-службой, то чтобы перекрыть доступ к ней, придется заблокировать весь Google (благодаря тому, как там организован хостинг сервисов).

Работы над DOH только начались, но уже вызвали существенный интерес... и ворчание касательно внедрения. Как на DOH отреагируют сети (и госструктуры), использующие DNS для выстраивания политик, покажет время.

Окостенение и смазка

Вернемся к вопросу «зачем менять Интернет». В своей работе разработчики протоколов снова и снова сталкиваются с одной и той же проблемой: сети делают некорректные предположения о трафике.

Например, у TLS 1.3 было немало проявившихся в последнюю минуту проблем с сетевыми приставками, которые принимали его за более раннюю версию протокола. А gQUIC заносит в черный список несколько сетей, которые задавливают трафик UDP, потому что считают его вредоносным или неприоритетным.

Когда протокол не может развиваться, потому что внедрение «заморозило» его точки развития, мы говорим, что он ***окостенел***. Одним из ярких примеров окостенения является TCP: множество сетевых приставок «позволяют себе вольности» в обращении с TCP — от блокировки пакетов с нераспознанными опциями TCP до «оптимизации» контроля перегрузки.

Для предотвращения окостенения важно открыть протоколам возможность развиваться в соответствии с потребностями Интернета будущего; иначе случится т.н. трагедия общин, где действия некоторых сетей – пусть и лишенные злого умысла – могут подорвать «здоровье» всего Интернета.

Предотвращать окостенение можно различными способами; если соответствующие данные шифруются, они недоступны никому, кроме обладателей ключа, что перекрывает возможность вмешательства. Если точка расширения не зашифрована, но обычно используется таким образом, который видимо «ломает» приложения (например, заголовки HTTP), вероятность вмешательства здесь ниже.

Там, где разработчики протоколов не могут использовать шифрование, а точка расширения используется нечасто, ситуации можно помочь, искусственно нагружая точку расширения; мы называем это ***смазкой***.

Например, QUIC поощряет использование на оконечных точках различных пустых значений при переговорах о версии (https://quicwg.github.io/base-drafts/draft-ietf-quic-transport.html#rfc.section.3.7), чтобы различные реализации не предполагали, будто номер версии не будет меняться (ситуация, обнаружившаяся в реализациях TLS и повлекшая много неприятных проблем).

Сеть и пользователь

Помимо борьбы с окостенением, эти изменения также отражают развитие отношений между сетями и их пользователями. Долгое время люди считали сеть благонамеренной или как минимум нейтральной стороной, но сейчас сетям перестали столь безоглядно доверять – и не только из-за сплошного мониторинга (https://tools.ietf.org/html/rfc7258), но и из-за атак типа Firesheep (http://codebutler.com/firesheep).

В результате возникает конфликт интересов между основной массой пользователей Интернета и теми из сетей, которым требуется доступ к данным, проходящим через них. Особенно выделяются здесь сети, которые желают налагать на своих пользователей определенные политики – например, корпоративные сети.

В некоторых случаях сети могут достичь своих целей, устанавливая на машины своих пользователей специальное ПО (или сертификаты CA, или браузерные расширения). Однако это не так просто, если компьютер пользователя не принадлежит сети или недоступен для нее: например, использование личных компьютеров и телефонов на работе стало общим местом, а устройства Интернета вещей редко оснащены адекватными интерфейсами управления.

В результате множество дискуссий в IETF о развитии протоколов вращается вокруг (часто конфликтующих) потребностей корпоративных и других «оконечных» сетей с одной стороны и Интернета в целом - с другой.

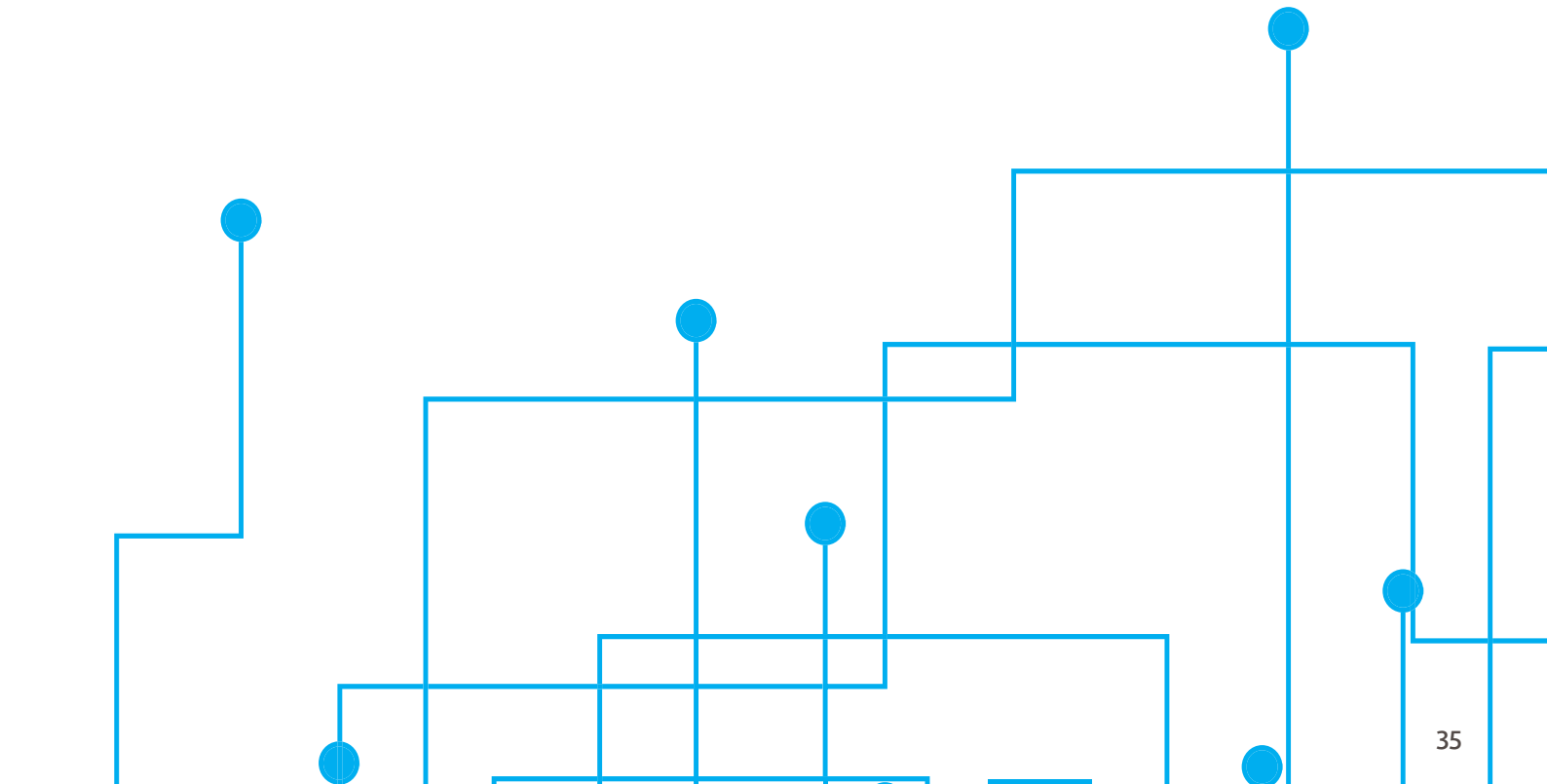
Примите участие в работе

Чтобы Интернет хорошо работал в долгосрочной перспективе, он должен приносить ценность конечным пользователям, не поддаваться окостенению и не мешать сетям работать. Изменения, происходящие сейчас, должны соответствовать всем трем перечисленным целям, но нам очень не хватает обратной связи от сетевых операторов.

Если предлагаемые изменения негативно скажутся на вашей сети – и даже если они на ней не скажутся, – пожалуйста, оставьте внизу свой комментарий, а еще лучше – примите участие в работе IETF (https://www.ietf.org/): посетите совещание, подпишитесь на рассылку или дайте обратную связь по проектам стандартов.

Автор выражает благодарность Мартину Томсону и Брайану Треммеллу за конструктивные замечания. Эта статья была впервые опубликована в блоге APNIC (https://blog.apnic.net/2017/12/12/internet-protocols-changing/).

Источник: Big Changes Ahead for Core Internet Protocols



Система доменных имен и предметное регулирование доменных споров

Мадина Касенова, Елена Воронина

В технологической архитектуре Интернета фундаментальную роль играют системы уникальных идентификаторов номеров: система адресов интернет-протокола (*IP-address*), система номеров автономных систем (*Autonomous System Numbers, ASN*), система параметров протоколов (*Protocol Parameters System*), система доменных имен (*Domain Name System, DNS*) и некоторых других. Функционирование названных уникальных систем обеспечивает возможность глобального объединения и коммуникации множества разнообразных сетей и устройств из любой точки мира в рамках единого глобального адресного пространства Интернета, предоставляя неограниченному кругу лиц, включая лиц, находящихся в разных правопорядках, взаимодействовать между собой.

К общим содержательным характеристикам систем уникальных идентификаторов Интернета следует отнести следующее. Во-первых, уникальные идентификаторы Интернета обладают нематериальной природой. Во-вторых, использование уникальных идентификаторов Интернета обеспечивается посредством механизма их трансграничного (глобального) распределения и регистрации. При этом «физически» инфраструктура уникальных идентификаторов Интернета характеризуется «технологической распределенностью», а обеспечение их функционирования поддерживается юридическими лицами, относящимися к разным правопорядкам, созданными в разных организационно-правовых формах и находящимися в разных юрисдикциях. Так, к примеру, региональные интернет-регистратуры (RIR) находятся в США (ARIN), Австралии (APNIC), государстве Маврикий (AfriNIC), Нидерландах (R IPE NCC) и Уругвае (LACNIC). Организации, являющиеся операторами корневых серверов DNS, расположены в США, Нидерландах, Швеции и Японии (http://root-servers.org/). В-третьих, распределение уникальных идентификаторов Интернета преимущественно реализуется в договорном порядке. В-четвертых, распределение уникальных идентификаторов Интернета не является основанием возникновения прав собственности на них, а регистрация распределения закрепляет право пользования на конкретный уникальный идентификатор Интернета.

Наряду с отмеченными общими характерными чертами, уникальные идентификаторы номеров и адресов Интернета обладают специфическими особенностями, которые обусловлены их объективными сущностными технологическими свойствами. При этом общие и специфические содержательные характеристики уникальных идентификаторов Интернета, особенности сложившегося порядка их использования во многом определяют сложности, к примеру, однозначного отнесения их к самостоятельным объектам гражданских прав, закрепления и регулирования форм их «правового существования», решения вопросов об их использовании «вне материальных носителей», установления режима использования и т.д.

Доменные имена

Система доменных имен (*Domain Name System, DNS*) наряду с обозначенными ранее общими содержательными характеристиками, присущими всем системам уникальных идентификаторов Интернета, обладает дополнительными специфическими особенностями. Система доменных имен (далее – DNS, система DNS)[1] как уникальный идентификатор Интернета отличает сеть Интернет от иных телекоммуникационных сетей.

Современная распределенная система доменных имен была предложена Джоном Постелом (*Postel J.*) и Полом Мокапетрисом (*Mockapetris P.*). В 1983 году в IETF (*Internet Engineering Task Force*, Инженерная группа проектирования Интернета)[2] были приняты два основополагающих нормативных документа, закрепивших концептуальные положения функционирования системы доменных имен и инфраструктурные особенности ее использования. Система DNS иерархически структурирована. Домен представляет собой область (ветвь) иерархического пространства доменных имен, обозначаемую уникальным доменным именем и обслуживаемую набором серверов DNS. В силу уникальности, невозможно «совместное» обладание доменным именем. Доменное имя – уникальный иерархический ряд символьного обозначения (меток – *Labels*), предназначенное для сетевой адресации; и в нем представлены различные уровни доменов, разделенные точками – «.». Каждое доменное имя «строится» в обратном порядке, начиная с корневой зоны (*Root Zone*), а точкой «.» отделяется верхний уровень иерархии. Часть иерархии в системе доменных имен занимают домены верхнего уровня, а крайняя правая метка в доменном имени является доменом верхнего уровня (*Top Level Domain, TLD*).

В иерархически структурированной системе доменных имен самую высокую позицию занимает «корневой домен»[3] и домены верхнего уровня, далее следуют домены последующих уровней (второго, третьего и т.д. уровня). Соответственно, каждый домен последующего уровня может создаваться только с использованием предыдущего доменного имени, а «исходным» является домен верхнего уровня. Таким образом, иерархия системы DNS представлена в самом доменном имени[4]; верхний уровень иерархии специфицирован «крайней правой точкой («.»), но часто эта завершающая точка опускается.

Технологическая иерархическая структурированность доменных имен объективирует «иерархическую» обусловленность порядка их распределения и регистрации в соответствующих реестрах, при этом речь идет о преимущественно договорном распределении доменных имен.

Регулирование вопросов «правового существования» доменных имен, их правовой статус, режим использования и т.д. в правопорядках различных государств определен по-разному. Вариативность регулирования зависит от того, игнорирует или учитывает законодатель технологическую специфику системы DNS, ее функциональную связанность с иными системами уникальных идентификаторов Интернета и их глобальный характер, положительно или отрицательно отвечает на ключевой вопрос о возможности регулирования отношений по поводу доменных имен исключительно на национальном уровне и т.д.

В праве зарубежных государств получило закрепление понятие «домен», «доменные имена», которые относятся к самостоятельным объектам прав, рассматриваются объектами прав *sui generis*, объектами неимущественных прав, не «приравниваемых» исключительно к объектам интеллектуальных прав[5], что представляется более адекватным подходом.

В российском праве понятия «домен», «доменное имя» не получили однозначного и единообразного закрепления, в равной степени как определение их содержания, правового статуса и режима и т.д.[6]. Так, понятие «домен» на законодательном уровне не закреплено, вместе с тем, к примеру, оно содержится в таком нормативном документе, как «Средства технические телематических служб. Общие технические требования» и определяется следующим образом: «иерархически структурированный глобальный адрес компьютера узла сети в виде строки символов»[7].

Понятие «доменное имя» закреплено в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и понимается как «обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет» (п. 15 ст. 2 ФЗ № 149-ФЗ)[8]. Вместе с тем, в «Правилах регистрации доменных имен в доменах *.ru* и *.рф*», принятых Координационным центром национального домена сети Интернет, определено несколько иначе, а именно: «символьное обозначение, предназначенное для сетевой адресации, в которой используется система доменных имен (DNS)». Кроме того, в названных документах дано понятие «домен», понимаемое как «область (ветвь) иерархического пространства доменных имен, обозначаемая уникальным доменным именем и обслуживаемая набором серверов»[9].

Гражданский кодекс РФ рассматривает доменные имена не в качестве самостоятельных объектов гражданских прав и средств индивидуализации[10]. Гражданский кодекс РФ упоминает доменные имена дважды: в контексте исключительного права на товарный знак (п. 5 ст. 1484 ГК РФ) и исключительного права использования наименования места происхождения товара (п.п. 4 п. 2 ст. 1519 ГК РФ)[11]. Несомненно, доменное имя обладает общими характерными чертами, сопоставимыми со средствами индивидуализации, однако не только не «исчерпывается» ими, но, в силу своей уникальности и технологических особенностей, обладает и *уникальными* отличительными признаками.

Представляется, что иерархическая организационная структурированность (уровневая детерминированность каждого последующего доменного имени от вышестоящего домена) и функциональная технологическая взаимосвязанность систем уникальных идентификаторов Интернета, к числу которых относится и система DNS, не должны игнорироваться, т.к. иной подход не будет способствовать адекватности правового регулирования использования доменных имен[12].

Домены верхнего уровня

Как отмечалось ранее, в иерархически структурированной системе DNS самую высокую позицию занимают уникальные домены верхнего уровня (*Top Level Domains, TLD*), которые создаются для государств и географических территорий, а также для конкретных сфер деятельности. В системе DNS существуют национальные домены верхнего уровня (*Country Top Level Domain, ccTLD*), общие, родовые домены верхнего уровня (*Generic Top-Level Domains, gTLD, genTLD*) и некоторые другие специальные домены.

В механизме делегирования и регистрации доменных имен верхнего уровня Корпорация Интернета по распределению имен и номеров (*Internet Corporation for Assigned Names and Numbers, ICANN*) занимает ключевое положение (далее – корпорация ICANN). С 2016 года техническое осуществление функции ведения базы данных (реестра) доменов верхнего уровня возложено на корпорацию «Публичные технические идентификаторы» (*Public Technical Identifiers, PTI*).

Названная корпорация (далее – корпорация PTI) является юридическим лицом, созданным по праву Калифорнии (США, г. Лос-Анжелес) в организационно-правовой форме публичной некоммерческой корпорации, единственным участником которой выступает корпорация ICANN[13].

Порядок создания и делегирования доменов верхнего уровня регулируется соответствующими документами-политиками корпорации ICANN и специфицируется в зависимости от типа доменов верхнего уровня. Вместе с тем, независимо от типа доменов верхнего уровня, их делегирование осуществляется конкретной национальной организации – администратору домена верхнего уровня.

Принципиально важное значение имеет закрепление в регулирующих документах корпорации ICANN нормативных положений о том, что использование доменных имен верхнего уровня не является основанием возникновения прав собственности на доменные имена; все права, возникающие у соответствующей организации, связываются с доверительным управлением делегированных доменов верхнего уровня; администратор, как доверительный управляющий, должен использовать доменные имена в «общественно-полезных целях»[14].

Домены верхнего уровня для стран, территорий, географических местностей *(Country Code Top Level Domain ccTLD)*

Названные домены верхнего уровня (далее – «домены *ccTLD*») в настоящее время рассматриваются как критически важный ресурс инфраструктуры государства[15]. Домены *ccTLD* являются идентификаторами стран, территорий, географических местностей. Национальные домены *ccTLD* являются двухбуквенными и соответствуют кодам стран, географических территорий и местностей, закрепленных в международном стандарте ISO 3166-1[16].

Наименование страны, территории или географической местности и их терминологическое написание согласовывается в рамках Организации Объединенных Наций (ООН)[17], однако для присвоения или отказа в присвоении домена ccTLD руководящим является классификатор ISO 3166-1. Например, к числу «непризнанных государств» относятся ряд стран: Абхазия, Косово, Северный Кипр, Нагорный Карабах, Палестина, Тайвань, Западная Сахара, Южная Осетия и др. В международном классификаторе ISO 3166-1 Палестина, Тайвань, Западная Сахара перечислены и им делегированы национальные домены ccTLD: Палестина – *.ps*; Тайвань – *.tw*; Западная Сахара – *.eh*. В настоящее время действует 259 доменов *ccTLD*[18].

Вместе с тем, если страна, географическая местность, территория не входит в международный классификатор ISO 3166, то национальный домен *ccTLD* может быть получен при вынесении положительного решения, принятого органом Организации Объединенных Наций. В соответствии с нормативными правилами Агентства по стандартам (ISO 3166/MA) Международной организации по стандартизации, государство или территория может быть включена также в Бюллетень названий стран ООН («Коды стран и регионов для статистического использования Статистического отдела ООН»). Условиями включения страны и территории в Бюллетень названий стран ООН являются следующие: 1) членство в ООН; 2) членство в любом из специализированных учреждений ООН; 3) участие в деятельности Международного суда ООН[19].

Домены *ccTLD* создаются и делегируются Администрацией адресного пространства Интернета (PTI/*IANA*) корпорации ICANN. Существенным моментом является то, что домены *ccTLD* присваиваются, делегируются безвозмездно, в рамках установленных корпорацией ICANN процедур, в заявительном порядке. Домены *ccTLD* создаются и делегируются соответствующей организации конкретного государства (администратор).

Несмотря на то, что домены *ccTLD* создаются и делегируются корпорацией ICANN, она не вправе самостоятельно принимать решение о создании новых доменов *ccTLD*, если страна или территория не включены в международный классификатор ISO 3166-1[20] либо Бюллетень названий стран ООН[21], и вправе отказать в регистрации. Однако «непризнанные» страны и территории не лишаются возможности «быть представленными» в Интернете. Официальные сайты «непризнанных стран и территорий» могут размещаться либо в зоне доменов *ccTLD* других стран, либо в зоне общих (родовых) доменов верхнего уровня. Например, сайт президента Южной Осетии размещается в зоне *.ru*[22]; сайт президента Нагорного Карабаха размещается в зоне *.am*[23]; сайт президента Северного Кипра размещается в зоне *.eu*[24].

В качества национальных организаций (администраторов) выступают юридические лица, созданные, в большинстве случаев, в организационно-правовой форме некоммерческих организаций. Национальные организации государств действуют в качестве администратора конкретного домена *ccTLD*. Например, в Российской Федерации администратором является Автономная некоммерческая организация «Координационный центр национального домена сети Интернет»[25].

Список доменов *ccTLD* и информация об администраторах, которым они делегированы, публикуется и находится в открытом доступе[26].

Наличие для каждого домена *ccTLD* администратора является ключевым требованием создания и делегирования соответствующего домена. Создание и делегирование домена *ccTLD* не связывается с обязательным требованием установления формальных договорных отношений с корпорацией ICANN[27], но на практике используются такие формы взаимоотношений, как обмен письмами (Австрия, Арабские Эмираты, Черногория и др.); заключение «меморандума о взаимопонимании» (Палестина, Молдова и др.)[28], заключение формального договора (Европейский Союз, Узбекистан и др.)[29].

Для доменов *ccTLD* основополагающими нормативными документами являются упомянутые ранее документы: RFC[30], политики и рекомендации корпорации ICANN[31], которые в том числе закрепляют отмеченное ранее положение о том, что использование доменов *ccTLD* не является основанием возникновения прав собственности на делегированные домены *ccTLD*; все возникающие права обусловлены тем, что администратор домена *ccTLD* является доверительным управляющим делегированных национальных доменов верхнего уровня и должен использовать эти доменные имена в «общественно-полезных целях».

Ряд государств обладают несколькими доменами *cTLD* (США, Великобритания, Норвегия, Китай, Россия, страны ЕС и др.). Например, в России действуют домены «*.ru*», «*.рф*».

Не все домены *ccTLD* «администрируются» национальными организациями государств. Так, администратором домена *ccTLD* государства Тувалу (*.tv*) выступает компания VeriSign Inc. – юридическое лицо права США, созданное в

соответствии с правом штата Делавэр; администратором домена *ccTLD* Туркменистана (*.tm*) с момента его создания (1997 г.) является английская компания *.TM Domain Registry Ltd.*[32]; в домене *ccTLD* Исландии (*.is*) располагается один из сайтов сервиса WHOIS – *www.who.is*.

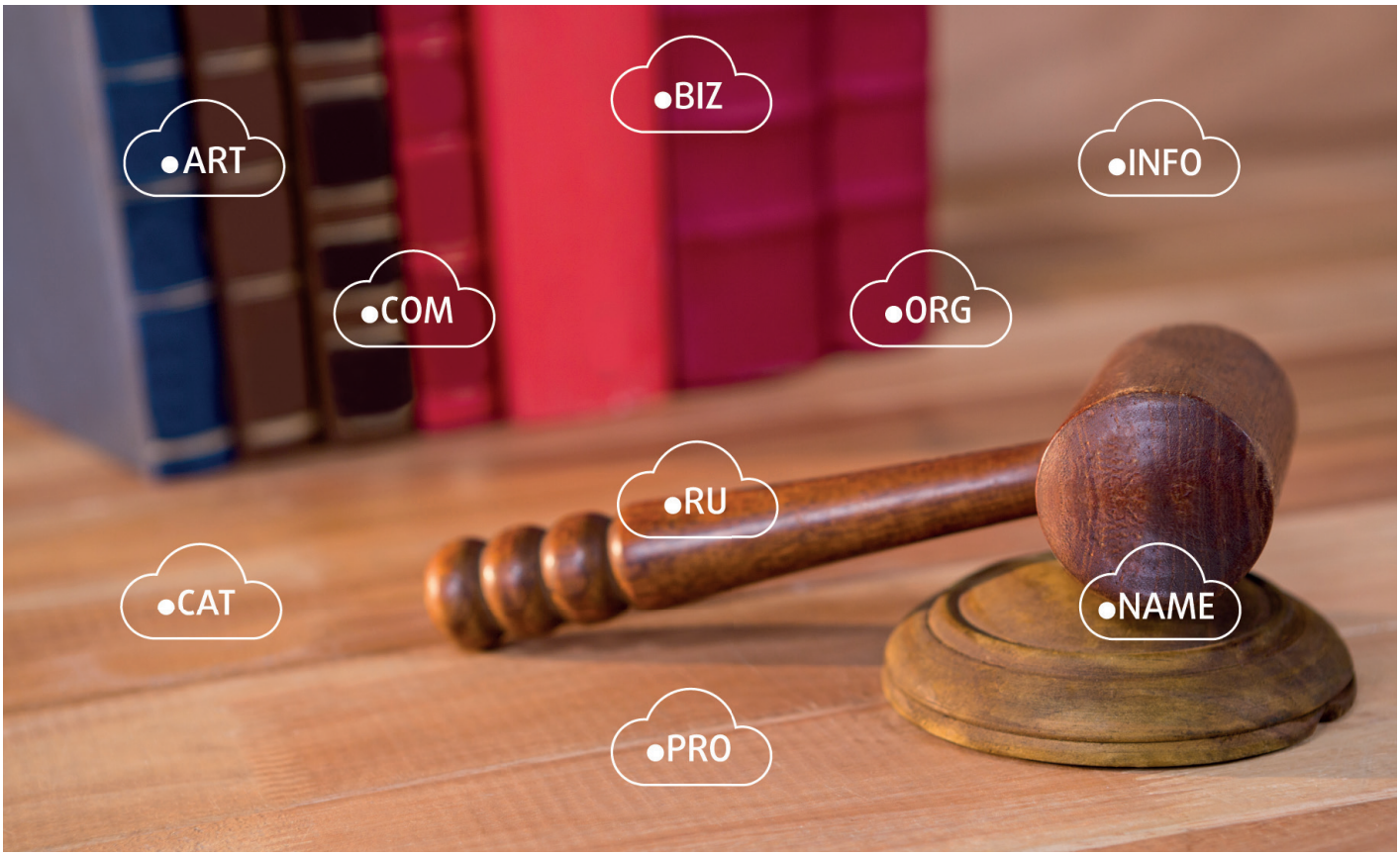
Порядок и условия использования зоны каждого домена *ccTLD* различаются, т.к. они определяются администратором этого домена и регистрируются по национальной процедуре[33]. Так, в Российской Федерации порядок и условия регистрации доменных имен и регулирующие отношения, возникающие в связи с регистрацией доменных имен второго уровня в домене *.ru*, определены администратором домена *ccTLD* – «Координационным центром национального домена сети Интернет». Основным документом являются «Правила регистрации доменных имен в доменах *.ru* и *.рф*» в редакции от 14 ноября 2017 года, действующие с 25 декабря 2017 года[34].

Трансграничное использование доменов *ccTLD* насчитывает более 30 лет, вместе с тем, на порядок их применения оказывают влияние политико-правовые факторы[35]. В настоящее время в качестве «элемента суверенности» государства рассматривается его «самоидентификация» в Интернете и наличие домена *ccTLD*. Тот факт, что государство представлено доменом *ccTLD*, несомненно, расширяет его возможности, прежде всего экономические[36].

Вместе с тем, существует ряд юридически сложных проблем использования доменов *ccTLD*. Нерешенными в правовом плане остаются такие вопросы: распространяется ли юрисдикция государства на всю зону домена *ccTLD*; является ли «трансграничным» спор, если отдельные территории государств обладают «своими» доменами *ccTLD*; сохраняет ли «юрисдикционное» значение домен *ccTLD*, если государство прекратило существование; сохраняет ли государство свою юрисдикцию в доменной зоне домена *ccTLD*, если администратором домена *ccTLD* не является юридическое лицо этого государства, и т.д[37]. Достаточно показательными являются следующие примеры.

Первый пример связан с тем, что в Китайской Народной Республике действует несколько доменов *ccTLD* – Китай (*.cn*); Гонконг (*.hk*), Макао (*.mo*), Тайвань (*.tw*), которые были получены в разное время. Однозначно нельзя ответить на вопрос о том, «распространяется ли юрисдикция» Китая на национальные зоны Гонконга, Макао, Тайваня, т.к. у каждого домена формально есть свой администратор, который вправе самостоятельно определять порядок и условия использования зоны каждого домена *ccTLD*. В 2007 году Тайвань инициировал в Швейцарии разбирательство в рамках гражданско-правовой процедуры против Международной организации по стандартизации (*ISO*) относительно переименования обозначения острова Тайвань. В международных стандартах наименование острова «Китайская республика Тайвань» переименовано в «Тайвань провинция Китая»[38]. Верховный Суд Швейцарии (*Swiss Federal Tribunal*) в 2010 году вынес решение об отказе рассмотрения гражданского иска Тайваня[39].

Второй пример имеет отношение к стандарту ISO 3166, который выбран в качестве критерия создания и делегирования доменов *ccTLD*. Этот стандарт был принят в «доинтернетовский» период (1974 г.) как единственный стандарт, где закреплялись коды стран и территорий. В 1997 году стандарт ISO 3166 был расширен и в него были включены три части: ISO 3166-1, который охватывал коды государств и зависимых территорий; ISO 3166-2,



включающий коды административных образований внутри государств (области, штаты, провинции); ISO 3166-3, который включал коды несуществующих государств (объединившиеся или распавшиеся государства, государства, сменившие названия)[40].

Применение в настоящее время международного стандарта ISO 3166 вызывает ряд спорных в юридическом плане проблем. Ранее отмеченный факт, что если страна или территория не включена в международный стандарт ISO 3166, то корпорация ICANN отказывает в создании и делегировании национального домена *ccTLD*[41]. Однако «спорные» моменты применения международного стандарта ISO 3166 призывы о его замене едва ли оправдывают, хотя бы на том основании, что не ясно, каким международным стандартом или иным «ресурсом» его можно заменить. Вместе с тем, «судьба стандарта ISO 3166», критерии делегирования доменов *ccTLD* и связанные с этими вопросами проблемы активно обсуждаются[42].

Родовые (общие) домены верхнего уровня *(Generic Top Level Domain, gTLD)* системы DNS

В систему DNS входят общие (родовые) домены верхнего уровня (*Generic Top-Level Domains, gTLD, genTLD*), не связанные с географическими или территориальными обозначениями и являющиеся специализированными доменами, относящимися к конкретной сфере деятельности. Общие (родовые) домены верхнего уровня (далее – «общие домены *gTLD*»), в отличие от доменов *ccTLD*, делегируются на основании заключения соответствующего договора с корпорацией ICANN, устанавливающей требования порядка их делегирования, регистрации в соответствующих реестрах Администрации адресного пространства Интернета (PTI/*IANA*) корпорации ICANN.

Число общих доменов с 1984 до 2001 года было ограничено семью (*.com, .org, .net, .edu, .int, .mil, .gov*); в связи с революционным ростом Интернета, корпорация ICANN утвердила использование еще семи новых общих доменов *gTLD* (*.info, .biz, .name, .coop, .museum, .aero, .pro*). В 2003 году были утверждены еще шесть доменов (*.cat, .mobi, .tel, .travel, .asia, .jobs*); с утверждением домена верхнего уровня *.xxx* и вводом его в эксплуатацию в 2011 году число общих доменов *gTLD* увеличилось до 21[43].

В целях повышения конкуренции использования интернет-технологий, расширения возможностей пользователей Интернета и т.д., в июне 2011 года правление корпорации ICANN утвердило Программу ввода в действие новых родовых доменов верхнего уровня (*New Generic Top Level Domains, new gTLD Program*)[44]. С 12 января 2012 года была открыта регистрация пользователей и подача заявок на новые общие домены верхнего уровня (*New Generic Top Level Domains, new gTLD*, далее – общие домены *new gTLD*). Расширение зоны доменных имен верхнего уровня практически не ограничивает доменное пространство Интернета, и в соответствии с принятыми процедурами, любое лицо вправе претендовать на получение общего домена *new gTLD*[45].

Примечательно, что США, как «Родина Интернета», *de facto* не использует национальный домен *ccTLD* и, как правило, правительственные (государственные) учреждения США используют общие домены *gTLD*, а именно: для правительства США – *.gov*; для учреждений военно-промышленного комплекса – *.mil*; для высших учебных и образовательных заведений – *.edu*.

Использование каждого общего домена *gTLD*, в отличие от доменов *ccTLD*, предполагает заключение договора между корпорацией ICANN и организацией, непосредственно занимающейся регистрацией доменов второго уровня (регистраторами) – «Договор об аккредитации регистратора» (*Registrar Accreditation Agreement*)[46], который по своей правовой природе является договором присоединения. В связи с тем, что сторонами таких договоров являются лица, являющиеся субъектами различных правопорядков, вопросы применимого права, порядок и процедура урегулирования споров регулируются условиями этого договора. В «Договоре об аккредитации регистратора» закреплена норма о том, что все споры с участием корпорации ICANN, связанные с этим договором или вытекающие из договора, относятся к юрисдикции США, и исключительным местом рассмотрения споров является суд Лос-Анджелеса, Калифорния (США). Обязательным условием, предусмотренным в названном договоре, является положение о предварительном применении досудебных процедур.

Как правило, в «Договоре об аккредитации регистратора» закреплено следующее условие о порядке урегулирования споров: «споры рассматриваются в суде компетентной юрисдикции или, по выбору любой из сторон, в арбитражном порядке в соответствии с Международным арбитражным регламентом американской Арбитражной ассоциации. Местом арбитражного разбирательства является г. Лос-Анджелес, Калифорния (США), языком разбирательства – английский язык».

Вместе с тем, в ряде договоров об аккредитации регистраторов содержится несколько иное условие о порядке урегулирования споров: «споры, возникающие в связи с договором или вытекающие из договора, подлежат обязательному арбитражному разбирательству, которое проводится в соответствии с правилами Международного арбитражного суда Международной торговой палаты. Местом арбитражного разбирательства является г. Лос-Анджелес, Калифорния (США), языком разбирательства – английский язык».

Следует отметить, что во многом дальнейшее развитие и порядок регулирования использования общих доменов *gTLD* обусловливается процессом внедрения новых общих доменов new *gTLD*, созданием доменов на национальных языках (интернационализированных доменных имен), как в зоне национальных доменов *ccTLD*, так и в общих доменах *gTLD*.

Расширение доменной зоны верхнего уровня в связи с введением в действие новых общих доменов *new gTLD* охватывает географические, культурные и лингвистические термины, такие как Африка, Берлин, Брюссель, Будапешт, Кейптаун, Москва, Нью-Йорк и др.[47], что приводит к расширению предметной сферы споров по доменным именам.

Достаточно показательным является пример «длящегося переговорного процесса» относительно рассмотрения заявки на новый общий домен *new gTLD* .amazon[48].

Правительственный консультативный комитет (GAC) корпорации ICANN, основываясь на предоставленных ему полномочиях, выдвинул возражения по заявке на новый общий домен верхнего уровня .amazon, поданный корпорацией Amazon[49]. Представители Бразилии и Перу, поддерживаемые другими представителями южноамериканских стран в правительственном консультативном комитете, выступили против делегирования названного домена и получили поддержку комитета.

Корпорация Amazon обжаловала решение по процедуре независимого пересмотра (*Independent Review Process*), в ходе которой было установлено, что заявка отклонена необоснованно, т.к. ни река Амазонка (Amazon), ни ее бассейн (Amazonia) не являются административными территориальными единицами, что могло бы послужить поводом для отказа от регистрации домена в пользу властей соответствующих территорий. Несмотря на то, что в Бразилии существует штат Амазонас (Amazonas), это название пишется иначе, чем «Amazon». Соответственно, слово «amazon» может быть использовано в качестве общего домена верхнего уровня без «одобрения» какой-либо страны/территории. В настоящее время руководство корпорации ICANN и корпорации Amazon пытаются найти компромиссное решение.

Доменные споры

Количество доменных споров увеличивается и затрагивает различные предметные сферы доменных имен. Большинство споров, возникающих в отношении доменных имен, связаны с доменными именами «второго уровня», т.к. в силу уникальности доменного имени, в одном домене верхнего уровня не может быть двух одинаковых доменных имен второго уровня. Имеется множество примеров споров в контексте конфликтов права на доменное имя и средства индивидуализации (товарные знаки, наименование мест происхождения товаров и т.д.); несоответствие доменного имени требованиям администратора доменного имени; передача доменного имени другому регистратору, неправомерное использование доменного имени (наряду с киберсквоттингом, в т.ч. мошенничество и злоупотребления, воздействующие на инфраструктуру) и т.д.

Красноречивым примером является дело «*Microsoft Corporation v. John Does*»[50], инициированное корпорацией Microsoft (истец) против пяти ответчиков (*5 John Doe Defendants*), имена которых не установлены (анонимные лица), действующих в так называемом ботнете («Dorknet»). Существо иска, как и решение суда, носит комплексный характер, и в рамках предмета настоящей статьи следует обратить внимание на то, что ответчики, в том числе: а) неправомерно использовали имена доменов Microsoft и иных третьих лиц; б) искажали либо скрывали информацию, идентифицирующую место (пункт) ее отправления или канал передачи коммерческого электронного сообщения; и с) прописывали ложную или вводящую в заблуждение информацию в адресной строке.

Суд вынес бессрочный судебный запрет (*Permanent Injunction*), в том числе указав, что «ответчики теряют свои имущественные права и контроль над предметными областями доменов, указанными в соответствующем приложении к решению суда»[51].

Разбирательство доменных споров осуществляется в различных юрисдикциях, как в судебном, так и во внесудебном порядке. Сложность рассмотрения доменных споров сопряжена с целым рядом нерешенных проблем, в ряду которых фрагментарность, неопределенность, «пробельность» правового регулирования на уровне национального права и отсутствие процесса его гармонизации, игнорирование объективных технологических свойств доменного имени и т.д. Кроме того, не всегда существует возможность выбора внесудебного порядка урегулирования доменного спора, в том числе с применением процедуры Единой политики разрешения доменных споров (*Uniform Domain Name Dispute Resolution Policy UDRP*) корпорации ICANN[52]. Обозначенные проблемы, в свою очередь, влияют на отсутствие единообразия правоприменительной практики при рассмотрении доменных споров.

Применительно к Российской Федерации следует отметить два принципиальных момента, связанных как с внесудебным, так и с судебным порядком разрешения доменных споров.

Во-первых, несмотря на то, что в России в среднем рассматривается не менее 60-90 доменных споров в год, упомянутая Единая политика разрешения доменных споров (далее – UDRP) для российских доменов зон *.ru* и *.рф* не применяется[53]. При этом достаточно быстро развивается система внесудебного разрешения доменных споров с применением процедуры UDRP на национальном и международном уровнях. На национальном уровне UDRP применяется, в частности, Азиатским центром разрешения доменных споров (*Asian Domain Name Dispute Resolution Centre*); Национальным арбитражным форумом (*The National Arbitration Forum*); Чешским арбитражным судом (*The Czech Arbitration Court*) и др.

На международном уровне UDRP применяется международной межправительственной организацией – Всемирной организацией интеллектуальной собственности (ВОИС) – в рамках Центра по арбитражу и посредничеству ВОИС[54].

Во-вторых, принципиально важным стала правовая позиция Суда по интеллектуальным правам относительно разрешения доменных споров. Речь идет о постановлении президиума Суда по интеллектуальным правам от 28.03.2014 №СП-21/4 «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров»[55], закрепившем использование положений UDRP, особо оговорив применение §4(a), 4(b) и 4(c) UDRP. Представляется, что принятие названного постановления будет способствовать формированию единообразия судебной практики, с учетом 15 места России в рейтинге стран происхождения ответчиков в рамках процедуры UDRP[56].

Заключение

Обобщая изложенное, можно отметить следующее:

- система доменных имен как глобальный уникальный идентификатор Интернета отличает сеть Интернет от иных телекоммуникационных сетей и «делает» уникальным Интернет как таковой;
- в настоящее время доменные имена так или иначе являются «доминирующим» объектом правового регулирования на национальном уровне. Вместе с тем, адекватность и эффективность правового регулирования определяется тем, что не игнорируется объективная технологическая связанность всех уникальных идентификаторов Интернета и иерархическая структурированность доменного имени; учитывается сложившийся, преимущественно договорный порядок распределения и регистрации доменов верхнего уровня;
- расширение доменной зоны увеличивает число доменных споров, предметная сфера которых многоаспектна и не исчерпывается исключительно интеллектуальными правами, связанными со средствами индивидуализации (товарными знаками, наименованиями мест происхождения товаров и проч.);
- с учетом глобального (трансграничного) функционирования уникальных идентификаторов Интернета, включая систему доменных имен, увеличение числа доменных споров выдвигает необходимость гармонизации понятийно-категориального аппарата и становится насущной потребностью.

Ссылки

1. Uniform Domain Name Dispute Resolution Policy (UDRP), *Наумов В. Б.* Процессуальный статус UDRP в России: возможности и парадоксы. http://russianlaw.net/law/law.htm UDRP в чистом виде в России не приживется. http://info.nic.ru/st/46/out_67.shtml *Страх А.* Юридические аспекты принятия UDRP в России. http://russianlaw.net/law/doc/a99.htm

2. Internet Engineering Task Force, IETF в русскоязычной версии переводится по-разному: Инженерный совет Интернета, Инженерная проектная группа Интернета, Рабочая группа по проектированию Интернета и т.д. IETF не является юридическим лицом и действует под эгидой Общества Интернета (ISOC). Русскоязычный перевод названия.

3. См. об этом, например, Internet Domain Name Registration. https://www.nic.ru/dns/service/new-gtld/#p1 (дата обращения: 15.09.2015)

4. *А. Робачевский*. Интернет изнутри. Экосистема глобальной Сети. 2-е изд. перераб. и дополн. – М.: Альпина Паблишер, 2017. С. 66-67.

5. См., например, *D. Lindsay*. International Domain Name Law: ICANN and the UDRP. Bloomsbury Publishing, 2007. – 512 P.; *Komaitis Konstantinos*. The Current State of Domain Name Regulation: Domain Names as Second Class Citizens in a Mark-Dominated World. Routledge, 2010 г. – 296 P. и др.

6. Вопрос о правовом регулировании доменных имен как объектов права получил отражение при разработке проекта части четвертой Гражданского кодекса РФ, в котором первоначально доменные имена рассматривались в качестве средств индивидуализации информационных ресурсов (с одновременным указанием на техническую функцию как средства адресации). Проект № 323423-4 Гражданского кодекса Российской Федерации. Часть четвертая. http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=323423-4&02 (дата обращения: 10.03.2018) См. также об этом подробнее: *Зыков С. В.* Об отнесении доменных имен к объектам интеллектуальных прав // Электронное приложение к «Российскому юридическому журналу». 2017. N 1. С. 72-78.

7. РД 45.134-2000 «Средства технические телематических служб. Общие технические требования». http://www.snip-info.ru/Rd_45_134-2000.htm

8. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 25.11.2017, с изм. и доп., вступ. в силу с 01.01.2018). СПС «Консультант Плюс».

9. Правила регистрации доменных имен в доменах *.ru* и *.рф*. https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf?v=5 (дата обращения: 10.03.2018); Правила регистрации доменных имен в домене *.su*. http://www.old.fid.su/su/registration/rules/ (дата обращения: 10.03.2018)

10. См. об этом подробнее: Доменные имена и товарные знаки в Рунете. 2017. https://cctld.ru/ru/domains/trademark/analytics/2017_11_OnLine_report_05_5.pdf (дата обращения: 10.03.2018); *Зыков С. В.* Об отнесении доменных имен к объектам интеллектуальных прав // Электронное приложение к «Российскому юридическому журналу». 2017. № 1. С. 72-78.

11. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 №230-ФЗ (ред. от 01.07.2017, с изм. и доп., вступ. в силу с 01.01.2018). СПС «Консультант Плюс».

12. Постановление президиума Суда по интеллектуальным правам от 28.03.2014 №СП-21/4 «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров». СПС «Консультант Плюс».

13. Документы корпорации ICANN. https://www.icann.org/public-comments/draft-pti-bylaws-2016-07-12-en Устав корпорации «Публичные технические идентификаторы» (Public Technical Identifiers, PTI). https://pti.icann.org/bylaws (дата обращения: 10.03.2018)

14. *Наумов В. Б.* Процессуальный статус UDRP в России: возможности и парадоксы. http://russianlaw.net/law/law.htm UDRP в чистом виде в России не приживется. http://info.nic.ru/st/46/out_67.shtml *Страх А.* Юридические аспекты принятия UDRP в России. http://russianlaw.net/law/doc/a99.htm

15. См. подробнее: *Arx K. G., Hagen G.R.* Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control // 9 Rich. J. L. & Tech. 4 (2002). http://www.law.richmond.edu/jolt/v9i1/article4.html (дата обращения: 10.03.2018) См. также: *Баринова Д.* Асимметрия политического пространства Интернета. http://www.intertrends.ru/twenty-fifth/010.htm; http://en.wikipedia.org/wiki/Country_code_top-level_domain&ei (дата обращения: 10.03.2018)

15. *Cukier K. N.* Eminent Domain: Initial Policy Perspectives on Nationalizing: Country-Code Internet Addresses, June 2002. http://www.cukier.com/inet02.html; а также *Баринова Д.* Национальные домены: символы государственных границ и безграничных возможностей. http://www.mgimo.ru/files2/y06_2010/155740/Barinova_domains.pdf (дата обращения: 10.03.2018) Государству или территории присваиваются новые коды в системе ASCII при смене названия, а числовой код меняется при изменении границ.

16. Country Codes - ISO 3166. http://www.iso.org/iso/country_codes.htm (дата обращения: 10.03.2018) Например, для стран двухбуквенные коды системы ASCII обозначены: *.uk* (Соединенное Королевство), *.de* (Германия), *.ru* (Россия), *.jp* (Япония), *.va* (Ватикан), *.au* (Австралия), *.mw* Малави. Национальные домены ccTLD: для территорий двухбуквенные коды системы ASCII обозначены: *.aq* (Антарктида), *.fc* (Остров Вознесения), *.eu* (Европейский Союз).

17. Коды соответствия стандарту ISO 3166 находятся в открытом доступе. https://www.iso.org/obp/ui/#search (дата обращения: 10.03.2018)

18. *Баринова Д.* Национальные домены: символы государственных границ и безграничных возможностей. http://www.mgimo.ru/files2/y06_2010/155740/Barinova_domains.pdf (дата обращения: 30.05.2015); *Баринова Д. С.* Национальные домены: роль государств в политическом пространстве Интернета: дис. ... канд. полит. наук. М., 2012.

19. Коды стран и регионов для статистического использования Статистического отдела ООН. http://1oodorog.ru/guide/articles/4396229/ (дата обращения: 10.03.2018)

20. ISO 3166-1 New access. http://www.iso.org/iso/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm (дата обращения: 10.03.2018)

21. *Баринова Д. С.* Национальные домены: символы государственных границ и безграничных возможностей // Вестник МГИМО-Университета. 2010. № 5. http://www.vestnik.mgimo.ru/fileserver/14/39_barinova.pdf (дата обращения: 10.03.2018)

22. О сайте президента Южной Осетии. http://presidentruo.org/?page_id=366 (дата обращения: 10.03.2018)

23. О сайте президента Нагорного Карабаха. http://www.president.nkr.am/rus/ (дата обращения: 10.03.2018)

24. *Баринова Д.* Национальные домены: символы государственных границ и безграничных возможностей. http://

mgimo.ru/files2/y06_2010/155740/Barinova_domains.pdf (дата обращения: 10.03.2018)

25. Координационный центр национального домена сети Интернет. http://www.cctld.ru/ru/about/charter.php (дата обращения: 10.03.2018)

26. См., например, User Instructions and Guides. https://www.iana.org/domains/root/help (дата обращения: 10.03.2018)

27. Delegating or redelegating a country-code top-level domain (ccTLD). https://www.iana.org/help/cctld-delegation (дата обращения: 10.03.2018)

28. Registry Agreements. https://www.icann.org/resources/pages/registries/registries-agreements-en (дата обращения: 10.03.2018)

29. Registry Agreements. https://www.icann.org/resources/pages/registries/registries-agreements-en (дата обращения: 10.03.2018)

30. RFC 1591. https://tools.ietf.org/html/rfc1591 (дата обращения: 10.03.2018)

31. User Documentation on Delegating and Redelegating Country-CodeTop-Level Domain, ccTLD; Principles for Delegation and Administration of Country Code Top Level Domains, GAC Principles; Framework of Interpretation of Current Policies and Guidelines Pertaining to the Delegation and Redeligation of Country-Code Top Level Domain Names и др. https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (дата обращения: 10.03.2018)

32. «.TM» Domain Registration. https://www.marcaria.com/ws/en/register/domains/bulk-domain-registration-extension-tm?curr=eur&gclid=CJPT5Jv1sMoCFWENcwodzDEIeQ (дата обращения: 30.05.2015)

33. Ряд организаций-регистраторов, аккредитованных корпорацией ICANN, помимо регистрации имен в доменах *.biz*, *.com*, *.info*, *.name*, *.net*, *.org*, оказывают регистрационные услуги в зоне различных национальных доменов (ccTLD). Список действующих TLD и данные администраторов, которым они делегированы, можно найти по адресу: http://www.iana.org/cctld/cctld.htm (дата обращения: 10.03.2018).

34. «Правила регистрации доменных имен в доменах *.ru* и *.рф*». https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf?v=5 (дата обращения: 10.03.2018)

35. См., например, *Баринова Д. С.* Национальные домены: символы государственных границ и безграничных возможностей // Вестник МГИМО-Университета. 2010. №5. http://www.vestnik.mgimo.ru/fileserver/14/39_barinova.pdf (дата обращения: 10.03.2018); «Теория и практика правового регулирования трансграничного функционирования и использования Интернета», М.: ИМИ МГИМО МИД России, 2015 и др.

36. Например, по данным Российской ассоциации электронных коммуникаций (РАЭК), совокупный оборот услуг в российском сегменте Интернета в 2014 г. достиг 1,43 триллиона рублей, и в 2015 г. ожидается рост в 20%. http://lenta.ru/news/2014/10/29/runet/ (дата обращения: 10.03.2018)

37. См., например, *Thunem H.* Domain name policy models among ccTLDs. http://www.isoc.org/educpillar/cctld/docs/RegistrationPoliciesUNINET-Sofia.pdf (дата обращения: 10.03.2018)

38. Switzerland; Taiwan: Against ISO over Request for Country Name Change Declined. http://www.bger.ch/fr/mm_5a_329_2009_d.pdf (дата обращения: 10.03.2018)

39. Taiwan Loses ISO Name Battle in Swiss Courts, GenevaLunch (Sept. 10, 2010). http://genevalunch.com/blog/2010/09/10/taiwan-loses-iso-name-battle-in-s; http://www.bger.ch/fr/mm_5a_329_2009_d.pdf (дата обращения: 10.03.2018)

40. Updates on ISO 3166. http://www.iso.org/iso/home/standards/country_codes/updates_on_iso_3166.htm?show=tab3 (дата обращения: 10.03.2018)

41. См. также Бюллетень названий стран ООН (Терминологический бюллетень ООН), № 347/Rev.1: «Названия стран». http://unstats.un.org/unsd/publication/SeriesM/SeriesM_49rev4corr4R.pdf (дата обращения: 10.03.2018)

42. См. в этом, например, Akkerhuis J. ISO 3166 Standard Role of the MA. https://ccnso.icann.org/sites/default/files/field-attached/presentation-iso-3166-31oct17-en.pdf (дата обращения: 10.03.2018)

43. Список зарегистрированных родовых доменов верхнего уровня. https://www.icann.org/resources/pages/listing-2012-02-25-en (дата обращения: 10.03.2018)

44. Все сопроводительные нормативно-правовые документы и информация о предпосылках, истории и развитии «Программы ввода в действие новых родовых доменов верхнего уровня» (New gTLD Program). http://gnso.icann.org/issues/new-gtlds/ (дата обращения: 10.03.2018)

45. Корпорация ICANN заключила несколько сотен договоров о регистрации общих доменов new gTLD и делегировала полномочия более чем на 200 общих доменов new gTLD. К примеру, общий домен new gTLD *.guru* превысил 50 тысяч доменов; *.club* – более 55 тысяч доменов. Список новых родовых доменов верхнего уровня. http://www.bb-online.com/newgtlds-domains.shtml (дата обращения: 10.03.2018)

46. Registrar Accreditation Agreement. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en (дата обращения: 10.03.2018) См. также, например, *Luk.* At EuroDNS, we value your rights to anonymity. https://www.eurodns.com/blog/privacy-matters-us (дата обращения: 10.03.2018)

47. *Mahler T.* Assessing Legal Risks of Closed Generic Top-Level Domains // European Journal of Law and Technology. Vol. 5. 2014. №3. http://unstats.un.org/unsd/geoinfo/ungegn/docs/28th-gegn-docs/WP/WP72_ICANN%20report.pdf (дата обращения: 10.03.2018)

48. Domain Incite. http://domainincite.com/22609-icann-chief-to-lead-talks-over-blocked-amazon-gtldhttps://cctld.ru/ru/press_center/digest/detail.php?ID=12141 (дата обращения: 10.03.2018)

49. Основание – «Руководство для Правительственного консультативного комитета по выдвижению возражений против ввода новых родовых доменов верхнего уровня» (Applicant Guide book Power for the GAC to Object new gTLD Application, GAC Guidebook) в редакции от 4 июня 2012 г.; INTA Internet Committee Comments on «The Protection of Geographic Names in the New gTLD Process». December 29, 2014. https://newgtlds.icann.org/en/applicants/gac-advice (дата обращения: 10.03.2018)

50. http://news.findlaw.com/hdocs/docs/cyberlaw/msdoes12061603cmp.pdf

51. Case 1:15-cv-06565-NGG-LB Document 33 Filed 03/31/17 Page 1 of 2 PageID #: 1359. Permanent Injunction&Order. United States District Court Eastern District of New York. https://botnetlegalnotice.com/dorkbot/files/perm_injunct_ordr.pdf

52. Об этом, к примеру, *Незнамов А. В.* Подведомственность доменных споров специализированным центрам в системе критериев национальной подведомственности // Арбитражный и гражданский процесс. 2010. №2. С. 11–14; *В. Наумов.* Процессуальный статус UDRP в России: возможности и парадоксы. http://russianlaw.net/law/law.htm; UDRP в чистом виде в России не приживется. http://info.nic.ru/st/46/out_67.shtml; *Страх А.* Юридические аспекты принятия UDRP в России. http://russianlaw.net/law/doc/a99.htm (дата обращения: 10.03.2018); Dispute Resolution Service Overview // Nominet. http://www.nominet.org.uk/disputes/drs/ (дата обращения: 10.03.2018) и др.

53. Доменные имена и товарные знаки в Рунете. 2017. С. 4. https://cctld.ru/ru/domains/trademark/analytics/2017_11_OnLine_report_05_5.pdf (дата обращения: 10.03.2018)

54. The Uniform Domain Name Dispute Resolution Policy and WIPO. http://wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf (дата обращения: 10.03.2018)

55. Постановление президиума Суда по интеллектуальным правам от 28.03.2014 №СП-21/4 «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров». СПС «Консультант Плюс».

56. Доменные имена и товарные знаки в Рунете. 2017. С. 4. https://cctld.ru/ru/domains/trademark/analytics/2017_11_OnLine_report_05_5.pdf (дата обращения: 10.03.2018)

Безопасность и приватность DNS для конечного пользователя

Бенно Оверайндер (Benno Overeinder)

Обеспечение сквозной защищенности данных осложняется самой природой Интернета. Это особенно актуально для DNS, со взаимодействия с которой начинается едва ли не каждое действие пользователя в Интернете. Тем не менее, открытые стандарты и работающий код доказывают, что безопасность и конфиденциальность для каждого – реально достижимы.

Повсеместное шифрование. Эта инициатива в техническом сообществе возникла в ответ на откровения Эдварда Сноудена о крупномасштабной слежке и мониторинге Интернета американскими спецслужбами. Отрезвляющий эффект от этой информации был таков, что массово начали разрабатываться и внедряться новые меры безопасности, такие как новый уровень шифрования для мобильных телефонов или службы защиты веб-трафика, такие как Let's Encrypt (https://letsencrypt.org/).

Все эти усилия направлены на то, чтобы на пути от пользователя до сервиса не оставалось лазеек для прослушивания. А значит, аутентификация и шифрование должны применяться уже на краю сети, т.е. у конечного пользователя. И поскольку едва ли не все действия в Интернете начинаются с запроса доменного имени, DNS занимает центральное место в обеспечении такой безопасности.

Предстоящую задачу простой не назовешь, так как мы умудрились превратить край сети, где обитает конечный пользователь, в крайне сложную и запутанную конструкцию: тут вам и NAT поверх Carrier Grade NAT, и брандмауэры, и мешанина IPv4/IPv6 с механизмами перевода между ними, и сетевые приставки, которые переписывают пакеты полностью или просто теряют их... Но во всей этой каше перед нами стоит две задачи, касающихся DNS:

1. Обеспечить подлинность и целостность данных DNS.
2. Защитить обмен данными между пользователем и DNS от посторонних ушей.

Проверку подлинности данных DNS берет на себя DNSSEC. Протокол DANE (DNS-based Authentication of Named Entities) позволяет произвести аутентификацию сервиса по открытому ключу (его также можно использовать для настройки сеанса TLS). С этой точки зрения ключевым компонентом для достижения полной и сквозной безопасности и конфиденциальности становится тупиковый резолвер DNS.

Хотя в инфраструктуре DNS тупиковый резолвер (stub resolver) считается простым компонентом, он должен работать и обеспечивать сквозную безопасность в описанной выше переусложненной среде. На приведенной ниже диаграмме виден уровень сложности служб DNS по сравнению с уровнем сложности сквозной безопасности.

Тупиковые резолверы должны иметь дело с самыми сложными на сегодняшний момент функциями сквозной безопасности, но не стоит забывать, что некоторые резолверы DNS не пересылают данные в формате DNSSEC дальше, что создает еще одну проблему.

Рассмотрим поподробнее описанные осложнения и варианты их решения.

Проблемы DNSSEC для оконечных точек

Здесь имеется множество различных проблем с проверкой DNSSEC и аутентификацией DANE. Мы не ставим своей целью осветить в этом разделе все ситуации, а взамен сосредоточимся лишь на важнейших.

Обход блокировок DNSSEC

Обход блокировок DNSSEC (DNSSEC Roadblock Avoidance) касается проверки DNSSEC в оконечных точках, которая зачастую бывает крайне затруднена из-за применения домашних маршрутизаторов и модемов (бюджетного класса), а также и других сетевых приставок на пути от оконечной точки до сервиса. Для решения этой задачи разработан документ

RFC8027 (https://tools.ietf.org/html/rfc8027), описывающий ряд сложных механизмов обращения к рекурсивным резолверам выше по потоку.

В оконечной точке применение этих методов поможет определить возможности рекурсивных резолверов выше по потоку и, если ни одно из промежуточных решений не сработает, применить резервную стратегию – задействовать собственный валидирующий резолвер, который будет опрашивать ответственные серверы имен непосредственно.

NAT64/DNS64

В нынешний переходный период между IPv4 и IPv6 инфраструктура DNS должна работать в ситуации, когда оконечные точки, поддерживающие только IPv6, обращаются к сервисам, поддерживающим (только) IPv4. Скорее всего, в обозримом будущем эта ситуация не изменится, поэтому здесь тоже необходимо надежное и основательное решение.

Для сред, в которых поддерживается только IPv6, NAT64 выполняет преобразование доступа к адресному пространству IPv4, сопоставляя эти адреса с адресами IPv6 с конкретным префиксом, а DNS64 выдает синтезированные адреса IPv6. Обратите внимание, что «обычный» DNS выдал бы IPv4-адрес службы. Очевидно, такие синтезированные сообщения DNS не являются подлинными и не пройдут проверку DNSSEC.

Чтобы можно было использовать DNSSEC в средах NAT64/DNS64, валидирующий тупиковый резолвер должен обнаружить, что находится в сети NAT64/DNS64, и выполнить синтез IPv6 самостоятельно, как описано в RFC7050(https://tools.ietf.org/html/rfc7050). Таким образом, оконечная точка, не поддерживающая IPv4, сможет проверять ответы DNS – подлинные адреса IPv4 – с помощью DNSSEC.

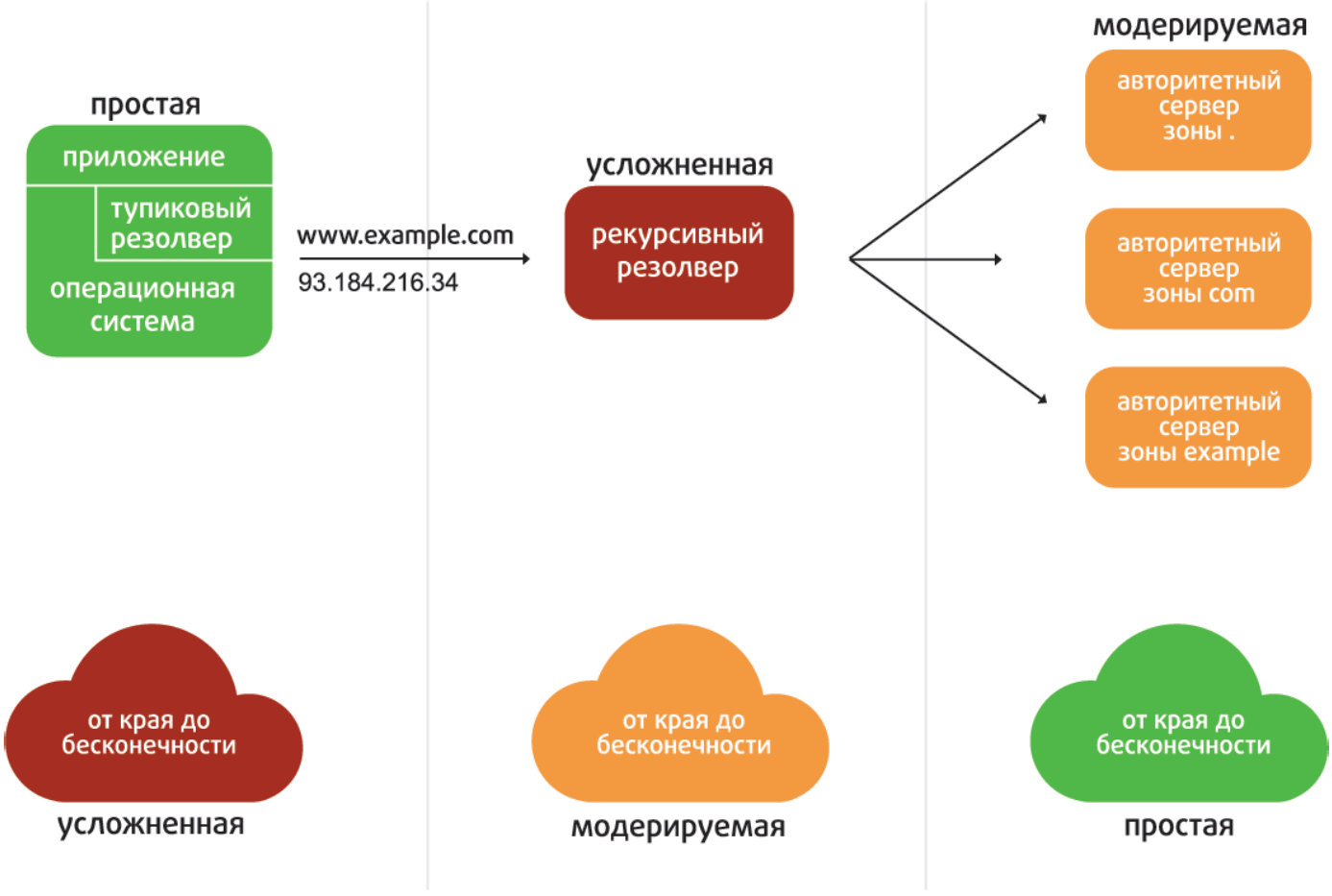
С момента создания RFC7050 возникла еще одна неожиданная ситуация, в которой от тупикового резолвера требуются подобные возможности, а именно, если ваше устройство настроено на работу с обеспечивающими приватность рекурсивными резолверами, такими как Quad9(https://www.quad9.net/), в мобильной или сотовой сети IPv6 без поддержки IPv4.

Поддержка точки доверия DNSSEC

Каждый раз, говоря о проверке DNSSEC, мы на самом деле говорим о проверке подписи, которой подписаны данные DNS. Проверка DNSSEC – это создание цепочки доверия, которая начинается с доверенного ключа DNSSEC и распространяется на ключ DNSSEC, которым подписывается ответ DNS.

Доверенный ключ DNSSEC, с которого начинается каждая проверка DNSSEC, называется точкой доверия (trust anchor) – как правило, это тот самый ключ, которым подписывается корневая зона (формально он называется ключом подписания корневых ключей – Root Key Signing Key).

Рис. 1. Уровень сложности служб DNS.



Управление точкой доверия жизненно важно для правильности работы валидирующих (тупиковых) резолверов DNSSEC. Поэтому появился документ RFC5011(https://tools.ietf.org/html/rfc5011), в котором предлагается отслеживать изменения точки доверия DNSSEC.

Разработчики этого документа исходили из того, что валидирующий резолвер – это непрерывно выполняемый процесс с правами системного администратора.

Проверка DANE выполняется на уровне приложения и использует тупиковый резолвер с пользовательскими привилегиями, как видно на диаграмме выше. Здесь нет никаких гарантий того, когда и в течение какого времени будет выполняться приложение тупикового резолвера, и полагаться на RFC5011 для отслеживания изменений точки доверия нельзя. Однако нет пока и стандартов, описывающих, как приложения должны поддерживать точку доверия. Один из методов для приложений пользовательского пространства называется DNSSEC с нулевой конфигурацией (zero-configuration DNSSEC) и основан на механизмах начальной загрузки точки доверия DNSSEC, описанных в RFC7958(https://tools.ietf.org/html/rfc7958). (Этот механизм разработан и применяется для getdns API, см. следующий раздел).

Путь вперед

Для адекватной безопасности и приватности первым условием является надежный тупиковый резолвер. В цепочке преобразования DNS тупиковый резолвер жизненно важен для выдачи проверенных на подлинность данных DNS и обеспечения приватности в оконечной точке.

API

Мы еще не касались вопроса о том, как предоставить проверенные данные DNS и проверку DANE приложению. Мы рассмотрели, как тупиковый резолвер может надежно получать проверенные данные DNSSEC, но пока не рассуждали о том, как приложение может получить к ним доступ. Необходимо дать разработчикам приложений простой в использовании и гибкий API.

Два свежих примера DNS API – это интерфейс systemd-resolved и проект getdns API.

Systemd использует systemd-resolved для реализации функционала DNS. Оба компонента являются частью проекта freedesktop.org(https://www.freedesktop.org/wiki/), и приложения могут использовать интерфейс D-Bus для полного доступа к systemd-resolved, например, в целях проверки DNSSEC.

Проект getdns API (https://getdnsapi.net/) совместно разрабатывается NLnet Labs(https://www.nlnetlabs.nl/). Цель проекта – создать гибкий и современный асинхронный DNS API для разработчиков приложений. При разработке API учитывались пожелания разработчиков приложений и систем, чтобы соответствовать потребностям и ожиданиям тех, кому, в конечном счете, придется с этим API работать.

В любом случае стандартизация DNS API и его доступность на различных платформах необходимы – так мы сможем улучшить нынешнюю ситуацию и добиться более массового распространения DNSSEC и DANE на рынке приложений.

Например, в проекте getdns API реализованы многие новейшие стандарты, направленные на то, чтобы сделать проверку DNSSEC и аутентификацию DANE доступными в оконечных точках: в частности, обход блоков DNSSEC, синтез IPv6 для сред NAT64/DNS64 и DNSSEC с нулевой конфигурацией.

Приватность DNS и DNS поверх TLS

Разработка и реализация getdns API также вплотную следует за развитием стандарта приватности DNS (DNS поверх TLS), описанного в RFC7858(https://tools.ietf.org/html/rfc7858). Этот механизм обеспечивает пользователю новый уровень безопасности, так как запросы DNS-клиента становятся невидимыми для пассивного наблюдателя. Однако стоит помнить, что все равно остается возможность утечки, поскольку ваши запросы и ответы на них известны не только вам. В системе, где между вами и авторитетными серверами DNS имеются посредники (резолверы), абсолютной конфиденциальности быть не может. Даже если вы будете направлять запросы авторитетным серверам DNS напрямую, они все равно будут знать, что вы запрашивали у них эту информацию. Поэтому имеет смысл внимательно изучить политику конфиденциальности вашего поставщика услуг DNS перед тем, как делать выбор.

getdns API обеспечивает приватность DNS для старых приложений посредством системного компонента Stubby (https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby). Он выполняется в виде демона на локальной машине, рассылая запросы DNS резолверам по зашифрованному соединению TLS.

Можно задать вопрос – чем это отличается от Unbound, другого проекта NLnet Labs: ведь он тоже может быть настроен как локальный транслятор пакетов, использующий DNS поверх TLS для пересылки запросов. В настоящий момент Unbound не обладает всем набором функционала TCP/TLS, реализованным в Stubby. Например, он не поддерживает режим Strict (https://tools.ietf.org/html/draft-ietf-dprive-dtls-and-tls-profiles) или паддинг запросов с целью маскировки размера пакета, а кроме того, он открывает отдельное соединение для каждого запроса DNS (Stubby использует соединения повторно).

В общем и целом, Unbound – более зрелый и стабильный демон, но мы стремимся сделать Stubby настолько же добротным. Обратите внимание, что оба демона можно использовать совместно: Unbound для кэширования, а Stubby – для канала TLS вверх по потоку (https://github.com/getdnsapi/stubby/issues/32).

И наконец, getdns API также удобен и полезен для разработчиков приложений на платформах Android и iOS. Защита данных и конфиденциальности для мобильных устройств в последующие годы приобретет особую остроту, и планы поддержки getdns API для этих платформ становятся все более конкретными.

DNS поверх HTTPS

Результатом недавней попытки IETF повысить целостность и конфиденциальность запросов DNS стал DNS поверх HTTPS E(https://tools.ietf.org/html/draft-hoffman-dns-over-https). Компонент конфиденциальности в DNS поверх HTTPS реализован, в сущности, путем создания зашифрованного канала TLS – ведь именно он отвечает за букву S в названии HTTPS, – и в этом смысле данное решение мало чем отличается от DNS поверх TLS. Похоже, само по себе оформление двоичного запроса DNS в виде HTTP не дает никаких новых преимуществ, но в этом решении имеется два интересных аспекта с точки зрения внедрения и приватности.

Как упоминалось выше, доставка данных DNSSEC в оконечные точки сопряжена со множеством трудностей: достаточно вспомнить и о потере пакетов при прохождении через неправильно функционирующие сетевые промежуточные устройства, и о резолверах, которые не пересылают данные DNSSEC дальше, и о многом другом. Иногда пакеты DNS прослушиваются или просто блокируются – вспомните гостиничные Captive-порталы, которые зачастую пропускают только веб-трафик и электронную почту. Потому DNS поверх HTTPS, использующий порт 443, наверняка найдет применение во многих ситуациях, где другие методы, такие как UDP или TLS, результата не дадут.

Второй момент – в процессе преобразования запросов DNS, например, при загрузке веб-страницы, происходит обращение к нескольким серверам DNS и соответственная утечка информации, добавляя в копилку повсеместного прослушивания. Минимизация имен запросов [RFC7816] (https://tools.ietf.org/html/rfc7816)помогает обеспечить конфиденциальность за счет того, что резолвер DNS отправляет ответственному серверу имен минимально необходимый объем информации. Но в DNS поверх HTTPS запросы DNS пересылаются вместе с трафиком HTTPS для загрузки веб-страниц. Дополнительным преимуществом перед минимизацией имен является то, что трафик DNS не сходит с пути, и потому меньше информации становится доступно третьим сторонам.

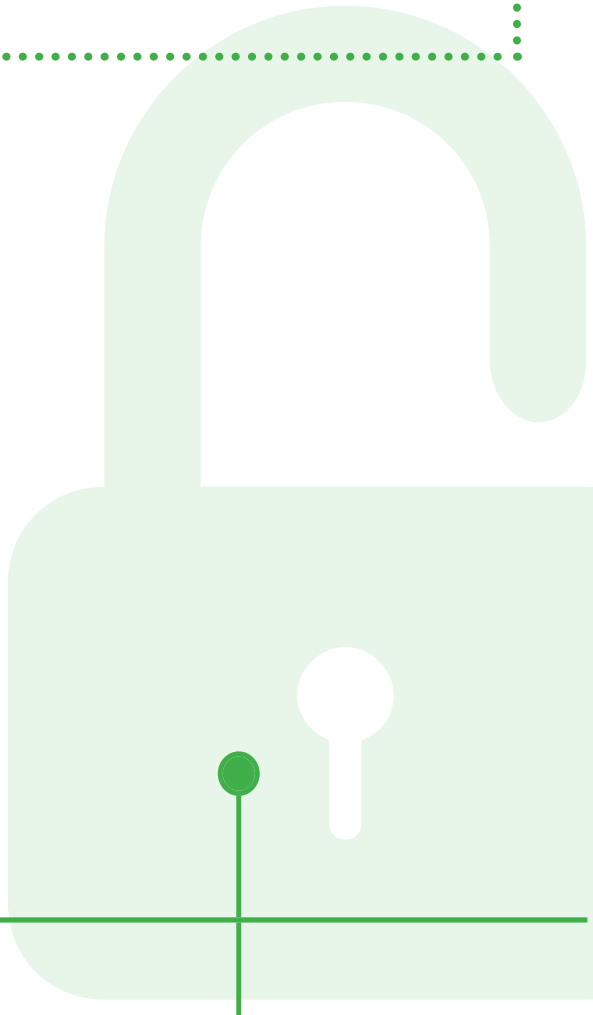
Источник: Bringing DNS Security and Privacy to the End User

Биография

Бенно Оверайндер (Benno Overeinder) – исполнительный директор нидерландской некоммерческой исследовательской компании NLnet Labs. Интересы Бенно лежат в средне- и долгосрочном планировании (стратегическом и тактическом) работы NLnet Labs, а помимо того – в области интернет-архитектуры, DNS, маршрутизации, стабильности и безопасности.

Заключение

По самой своей природе Интернет растет, развивается и совершенствуется таким образом, что его среда не может оказаться простой. Это осложняет его защиту, но открытые стандарты и работающий код доказывают, что безопасность и конфиденциальность для каждого – реально достижимы.



Новости Доменной индустрии

Важные события 2017-2018

ЛУЧШИМ БОРЦОМ ЗА БЕЗОПАСНОСТЬ РУНЕТА ПРИЗНАНА КОМПАНИЯ «БИЗОН»

14.12.2017

Лауреат в номинации «Безопасность Рунета»

14 декабря в Технопарке «Сколково» состоялась церемония вручения второй ежегодной премии «Цифровые вершины», которая прошла при поддержке Координационного центра доменов .RU/.РФ. КЦ также учредил собственную номинацию «Безопасность Рунета».

Лауреатом в номинации «Безопасность Рунета» стала компания «БИЗон», которая занимается анализом киберугроз и тестированием систем безопасности крупнейших кредитных организаций, проведением экспертиз, связанных с киберрисками. В 2016 году компания присоединилась к работе проекта «Нетоскоп», а также заключила с Координационным центром доменов .RU/.РФ соглашение о работе в качестве компетентной организации. Награду из рук директора Координационного центра **Андрея Воробьева** получил директор компании «БИЗон» **Дмитрий Самарцев**.

Компания «БИЗон» специализируется на вопросах фишинга и выявления сайтов, нарушающих законодательство в области информационной безопасности в финансовом секторе. В 2017 году компанией было направлено около 700 обращений к регистраторам о снятии с делегирования доменных имен, замеченных в фишинге. Внимание к обеспечению информационной безопасности в области банковских услуг стало одной из главных примет уходящего года.

ВИНТ СЕРФ: ГЛАВНОЙ ЗАДАЧЕЙ ЧЕЛОВЕЧЕСТВА БУДЕТ ПРЕДОТВРАЩЕНИЕ ФРАГМЕНТАЦИИ ИНТЕРНЕТА

19.12.2017

18 декабря в Женеве в европейской штаб-квартире ООН начал работу XII Всемирный форум по управлению Интернетом. В мероприятии приняли участие все заинтересованные стороны, которые вносят свой вклад в развитие Интернета – представители международных организаций, администраций связи разных стран, академического и технического сообщества, институтов гражданского общества и бизнеса.

IGF в Женеве

На открывающей сессии прошло выступление одного из основателей Интернета, вице-президента Google Винта Серфа, который сделал несколько прогнозов о том, каким Интернет будет в 2027 году. По его словам, к этому времени к сети будут подключены по меньшей мере шесть миллиардов человек, основная дискуссия будет вестись вокруг вопросов информационной безопасности и стабильности работы Интернета и, наконец, главной задачей человечества в отношении Интернета будет поддержание его единства и предотвращение фрагментации.

В ПРОЕКТЕ «НЕТОСКОП» ПОЯВИЛИСЬ ИНОСТРАННЫЕ УЧАСТНИКИ

18.12.2017

В 2017 году к проекту «Нетоскоп» присоединились сразу четыре новых участника. Это компании SURFnet, iThreat Cyber Group Inc., SkyDNS и Ассоциация участников «МастерКард». Примечательно, что две компании – иностранные, так что проект «Нетоскоп» выходит на новый для себя международный уровень.

Нетоскоп

Одной из специализаций исследовательского центра SURFnet (Нидерланды), связанной с доменной индустрией, является анализ «репутации» доменных зон. Компания давно является признанным лидером в этой области: например, уже несколько лет SURFnet выполняет работы по определению индикаторов «здоровья» доменных зон в рамках контракта с ICANN. Американская компания iThreat Cyber Group Inc. с 1997 года занимается анализом стабильности и безопасности системы DNS. Генеральный директор компании Джеффри Бедсер является постоянным членом комитета по безопасности и стабильности ICANN. Соглашение с Координационным центром доменов .RU/.РФ подписали и две российские организации: крупный DNS-провайдер SkyDNS, предоставляющий услуги интернет-безопасности и контент-фильтрации, и Ассоциация участников MasterCard. Здесь основным направлением сотрудничества станет противодействие мошенничеству с кредитными картами и платежными системами, в первую очередь это касается противодействия фишингу.

ФУНКЦИИ «ТЕХНИЧЕСКОГО ЦЕНТРА ИНТЕРНЕТ» ПЕРЕДАЮТСЯ ДОЧЕРНЕЙ КОМПАНИИ ПАО «РОСТЕЛЕКОМ»

24.01.2018

Общее собрание учредителей Координационного центра доменов .RU/.РФ приняло решение о передаче функций Технического центра (оператора реестров) национальных доменов .ru/.рф в структуры Группы компаний ПАО «Ростелеком». Для обеспечения целостности, непрерывности, стабильности, устойчивости и защищенности функционирования российского сегмента сети Интернет и его критической инфраструктуры учреждена специальная организация – Общество с ограниченной ответственностью «Технический центр Интернет», являющееся дочерней структурой компании ООО «РТК – Центр обработки данных». ООО «РТК-ЦОД» – центр компетенции ГК ПАО «Ростелеком» в области услуг центров обработки данных, облачных сервисов и сетевых технологий.

Данное решение было принято по предложению Минкомсвязи РФ о передаче поддержки реестров национальных доменов .ru и .рф специализированной дочерней компании ПАО «Ростелеком». Передача поддержки в новую организацию дополнительно повысит надежность, стабильность и устойчивость работы реестров. В ООО «ТЦИ» по согласованию сторон будут переданы все лучшие наработки и технологии «Технического центра Интернет», а также высококвалифицированные кадры, которые сегодня работают в АО «ТЦИ».

ЗЛОУМЫШЛЕННИКИ ИСПОЛЬЗУЮТ ДАЖЕ НЕЗАРЕГИСТРИРОВАННЫЕ ДОМЕНЫ

02.02.2018

1 февраля в Москве открылся «Инфофорум 2018», где собрались представители государственной власти и ведущие российские эксперты в области информационной безопасности, борьбы с киберпреступностью, создания систем обеспечения информационной безопасности. Одна из основных целей Инфофорума, который проводится уже в 20-й раз, – это усиление взаимодействия специалистов в области обеспечения национальной инфобезопасности. В 2018 году в форуме приняли участие более 1600 человек.

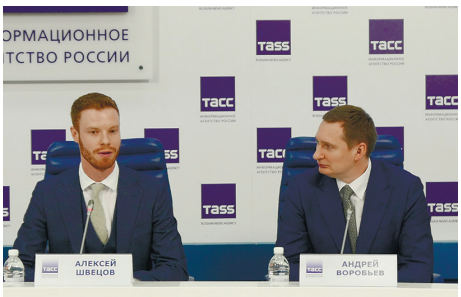
«Инфофорум 2018»

Координационный центр доменов .RU/.РФ выступил партнером тематического заседания «Безопасный Интернет». Эксперты КЦ рассказали о новых видах угроз, с которыми столкнулись при анализе зловредных доменов: «Одной из главных тенденций 2017 года стало использование в противоправных целях доменов, которые даже не зарегистрированы. Зловредное программное обеспечение, которое заражает компьютеры пользователей, содержит автоматически сгенерированные доменные имена, информации о которых еще нет в реестре. Запросы на эти доменные имена создают подобие DDoS-атаки на систему DNS – большое количество ответов о несуществующем домене приводит к большим нагрузкам на серверы. В дальнейшем эти доменные имена могут быть зарегистрированы и использоваться для управления бот-сетью и обновления зловредного программного обеспечения», – рассказал Михаил Анисимов, заместитель начальника отдела внешних коммуникаций. Также он отметил, что сегодня регистратуры доменов верхнего уровня совместно с экспертами в сфере информационной безопасности разрабатывают эффективные механизмы противодействия этому явлению.

«НЕТОСКОП» ПОМОЖЕТ FIFA БОРОТЬСЯ С МОШЕННИЧЕСТВОМ ПРИ ПРОДАЖЕ БИЛЕТОВ НА ЧМ-2018

13.02.2018

FIFA и Координационный центр доменов .RU/.РФ заключили соглашение о включении FIFA в состав участников научно-технического сотрудничества «Нетоскоп», призванного обеспечивать безопасность в области использования доменных имен. FIFA будет передавать данные о доменах, которые используются для фишинга при нелегальной продаже билетов на Чемпионат мира по футболу FIFA 2018 года в России.



FIFA и Координационный центр доменов .RU/.РФ

Другие организации, участвующие в «Нетоскопе», также занимаются вопросами борьбы с фишингом. Специализация FIFA в рамках проекта – это выявление в Рунете случаев неправомерной торговли билетами на ЧМ-2018 без заключения договора с организаторами турнира и передача информации о таких нелегальных ресурсах в «Нетоскоп». Далее полученная от FIFA информация о подозрительных сайтах будет проанализирована участниками проекта «Нетоскоп», и в случае подтверждения незаконной деятельности, ресурсы будут заблокированы. Вопросы мошенничества при продаже билетов по мере приближения начала чемпионата становятся все более актуальными, и присоединение FIFA к «Нетоскопу» – своевременная мера, направленная прежде всего на защиту интересов болельщиков.

Календарь событий: 2018 год

Международные события

29 апреля - 11 мая,
AfNOG/AIS/AfriNIC,
Дакар, Сенегал

AFRINIC является одной из пяти интернет-регистратур (RIR) и проводит две открытые встречи каждый год в различных местах по всему региону обслуживания. Встречи AFRINIC предоставляют уникальную возможность для лиц и организаций, связанных с Интернетом, собираться для обсуждения политик, регулирующих распределение номерных интернет-ресурсов в африканском регионе, для обмена техническими знаниями и участия в семинарах и учебниках. https://www.internetsummit.africa/

14-18 мая,
RIPE 76,
Марсель, Франция

Встречи RIPE проводятся два раза в год и собирают более 500 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Встреча длится 5 дней и начинается с двухдневной пленарной программы, за которой следуют несколько параллельных сессий заседаний рабочих групп. https://ripe76.ripe.net/

22-27 июня,
ICANN 62,
Панама

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. Участие во встречах ICANN бесплатно.
https://meetings.icann.org/en/calendar

25-27 июня,
NANOG 73,
Денвер, США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG на технологиях и системах, обеспечивающих работу Интернета: системе глобальной маршрутизации, DNS, пиринге и связности. NANOG имеет активный список рассылки и проводит конференции три раза в год. Поскольку инженерные вопросы NANOG имеют глобальный характер, участие в списке рассылки и конференциях может быть полезно широкому кругу технических специалистов в области сетевых технологий Интернета. Подача заявок на доклады заканчивается 8 мая 2018 г.
https://www.nanog.org/meetings/NANOG73

14-20 июля,
IETF 102,
Монреаль, Канада

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания, на которые приезжают разработчики протоколов, инженеры и операторы со всего мира (в среднем около 1200 участников из более 50 стран мира). Совещания IETF - это хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке. https://www.ietf.org/how/meetings/upcoming/102/

В России

3 апреля,
Екатеринбург

День MSK-IX в Екатеринбурге
Ежегодное место обсуждения последних тенденций в области связи и передачи данных.
https://www.msk-ix.ru/ix/ekt/

17 апреля,
Новосибирск

День MSK-IX в Новосибирске
Ежегодная встреча представителей ведущих интернет-операторов, провайдеров в Новосибирске.
https://www.msk-ix.ru/ix/nsk/

24-25 мая,
Казань,
отель «Корстон»

IT&Security Forum 2018
ITSF - одно из крупнейших событий отрасли информационных технологий и кибербезопасности в регионе. http://itsecurityforum.ru/

31 мая,
Владивосток,
конференц-центр
отеля «Акфес-Сейо»

BIT-2018 во Владивостоке
Международный Форум «Вокруг облака. Вокруг ЦОД. Вокруг IP. Вокруг данных. Вокруг IoT» (или BIT-2018). Это уникальное отраслевое мероприятие, отличающееся комплексным подходом, качеством информационного наполнения и неповторимой атмосферой, объединит лучших представителей ИКТ-сообщества и бизнес-среды региона. https://vladivostok-2018.ciseventsgroup.com/mesto-provedeniya.html

6-8 июня,
Казань,
Иннополис

ЦИПР 2018
Конференция ЦИПР - межотраслевая площадка, созданная для консолидации отрасли и обеспечения глобального диалога представителей промышленности, профессионалов отрасли ИКТ, оборонного комплекса, инвесторов и государства по самым острым и актуальным вопросам развития цифровой экономики, несырьевого экспорта, конверсии в ОПК и обеспечения кибербезопасности. http://cipr.ru/

В Москве

11-12 апреля,
Radisson Royal Hotel

Capacity Russia & CIS 2018
Крупнейшее телекоммуникационное событие в регионе, объединяющее российских и международных операторов связи, центры обработки данных, облачных провайдеров, компании IXP. Более 130 компаний-участниц из более чем 50 стран.
http://www.capacityconferences.com/Capacity-Russia-CIS

17 апреля,
«Лотте Отель
Москва»

Телеком 2018
В мероприятии примут участие ведущие игроки телекоммуникационного рынка: представители и руководители крупнейших телеком-компаний России и зарубежья, а также MVNO-операторов, органов государственной власти, банков, OTT-сервисов, технологических и интернет-компаний, операторов цифрового телевидения и Интернета, а также инвесторы, аналитики и эксперты отрасли. https://events.vedomosti.ru/events/telekom18

24 апреля,
Экспоцентр

Связь 2018
На выставке широко представлены решения для фиксированной, сотовой, спутниковой и волоконно-оптической связи, сетей передачи данных, телекоммуникационное, серверное и сетевое оборудование, системы телевещания, решения в области информационной безопасности, виртуализации, интернет-технологии. А также обширная деловая программа Большого медиа-коммуникационного форума. http://www.sviaz-expo.ru/

30-31 мая,
отель Hilton Garden Inn Moscow
Krasnoselskaya

Wireless Russia & CIS Forum
10-й Международный бизнес-форум. LTE, 5G & Beyond – рынок мобильной связи в эпоху запуска сетей пятого поколения и масштабного расширения Интернета вещей (IoT).
http://www.comnews-conferences.ru/ru/conference/wireless2018

4-5 июня,
Гранд-отель Marriott

ENOG 15 / RIPE NCC
ENOG - региональный форум, где интернет-специалисты, занимающиеся важнейшими аспектами работы Интернета, обмениваются знаниями и опытом по темам, актуальным для России, СНГ и Восточной Европы. https://www.enog.org/enog-15/

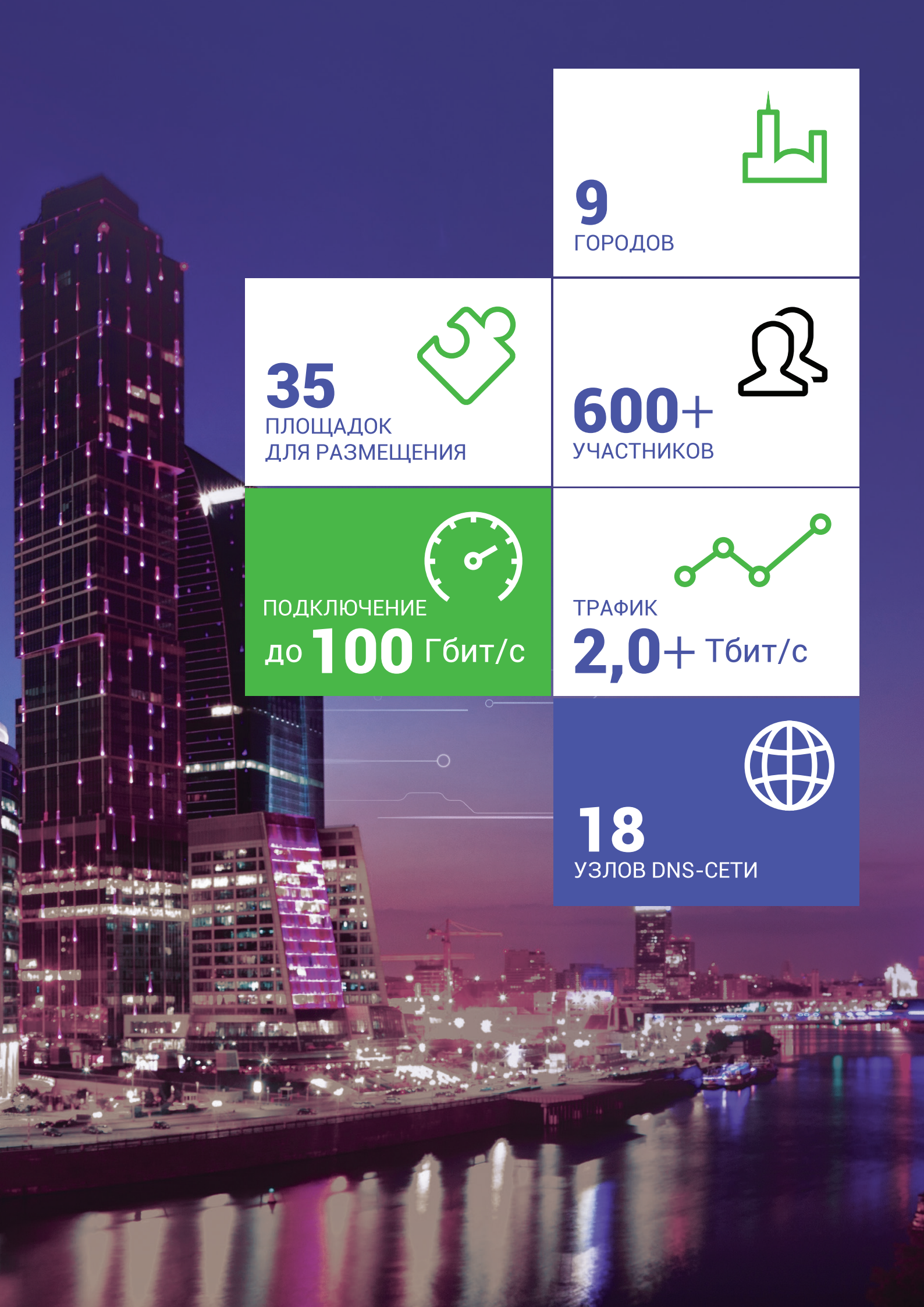
20 июня,
Holiday Inn Lesnaya

Future of Telecom 2018
Седьмой Ежегодный форум "Future of Telecom: Business Models & Strategies. Точки роста". Перспективы на традиционном и на нетелеком-рынках. Новые возможности для удержания абонентов и оптимизации расходов. Новые возможности для оператора: Internet of Things. Machine Learning. Enterprise Mobility. Мобильные финансы. Cloud. OTT. BigData & Analytics. InfoSecurity / Blockchain as a Service и др. http://telco-forum.ru/

MSK IX

WWW.MSK-IX.RU

+7 (495) 737-9295



9
ГОРОДОВ

35
ПЛОЩАДОК
ДЛЯ РАЗМЕЩЕНИЯ

600+
УЧАСТНИКОВ

ПОДКЛЮЧЕНИЕ
до **100** Гбит/с

ТРАФИК
2,0+ Тбит/с

18
УЗЛОВ DNS-СЕТИ

Интернет изнутри

2018