ICANN81 | AGM – Совместное заседание: GAC и RSSAC
Воскресенье, 10 ноября 2024 г. - 9:00 - 10:00 TRT

JULIA CHARBELIN: Здравствуйте и добро пожаловать на совместное заседание GAC и RSSAC. Меня зовут Джулия Шарволен (Julia Charvolen) из группы поддержки ICANN в GAC. Пожалуйста, обратите внимание, что эта сессия записывается и регулируется ожидаемыми стандартами поведения ICANN и политикой сообщества ICANN по борьбе с домогательством. Во время сессии вопросы и комментарии будут зачитываться вслух только в том случае, если они будут заданы в чате. Перевод на этой сессии будет осуществляться на все шесть языков ООН и португальский. Если вы хотите выступить на этом заседании, пожалуйста, поднимите руку в Zoom. Пожалуйста, назовите свое имя и язык, на котором вы будете говорить, если это не английский, и не забывайте говорить в разумном темпе. Сейчас я передаю слово Нико Кабальеро (Nico Caballero), председателю GAC. Пожалуйста.

NICO CABALLERO: Большое спасибо, Джулия. Приветствую всех. Как некоторые из вас были проинформированы через ежедневную рассылку и другие каналы связи для участников ICANN 81, каждый год 10 ноября жители Турции соблюдают минуту молчания в 9:05 утра в память о смерти великого исторического лидера страны, Мустафы

Кемаля Ататюрка, основателя Турецкой Республики. В связи с этой памятной датой мы немного отложим начало сессии на несколько минут, точнее, на пять минут, и начнем в 9:10 утра по местному времени. Я ценю, что наш докладчик, председатель RSSAC JEFF OSBORN (Jeff Osborn), присоединился к нам в связи с этим небольшим изменением времени начала. Спасибо, Джефф, и спасибо, Роб, за это. Так что, пожалуйста, не стесняйтесь молча наблюдать за этим обычаем. Мне сказали, что мы, скорее всего, услышим звуковой сигнал момента незадолго до минуты поминовения. Поэтому мы начнем в 9:10, чтобы людям, покидающим зал, было удобно вернуться. Итак, позвольте мне еще раз поприветствовать вас. Сейчас 9:02. Так что примерно через три минуты мы должны услышать сирену, или я не знаю точно, как она работает, но не удивляйтесь. Добро пожаловать, Джефф, добро пожаловать, Роб. Доброе утро.

JEFF OSBORN: Я надеюсь, что получу сигнал от моего уважаемого коллеги, г-на Кабальеро, о том, что пора заканчивать, так что спасибо вам за это. Доброе утро всем, кто находится в Стамбуле, или добрый день, добрый день и добрый вечер тем, кто присоединился к нам удаленно. Меня зовут Джефф Осборн (Jeff Osborn), и я являюсь председателем RSSAC, Консультативного комитета по системе корневых серверов в ICANN. На своей основной работе я являюсь президентом компании ISC, разработчика программного обеспечения с открытым исходным кодом для DNS и других интернет-протоколов. Я ценю возможность поговорить с вами

сегодня, и я надеюсь на продолжение дискуссии между членами RSSAC и GAC. Я надеюсь, что это начало длительного диалога, а не просто одноразовое знакомство с RSSAC, системой корневых серверов и самой системой доменных имен. Основываясь на отзывах GAC, сегодня мы будем представлять информацию в двух частях. В первой части рассказывается о Консультативном комитете по системе корневых серверов и о том, как он работает в системе ICANN с участием многих заинтересованных сторон, а во второй - о системе доменных имен и системе корневых серверов. Мы надеемся, что это будет информативно и познавательно, и я с нетерпением жду ваших вопросов в конце.

NICO CABALLERO: Спасибо всем за соблюдение этих трех минут молчания.

JEFF OSBORN: Часть 1, Консультативный комитет по системе корневых серверов. RSSAC имеет очень узкую сферу деятельности и цель, показанную здесь, которую сообщество ICANN нам определило в своих уставах. На экране вы можете видеть, что сфера деятельности заключается в консультировании сообщества ICANN и Правления по вопросам, связанным с работой, администрированием, безопасностью и целостностью системы корневых серверов Интернета.

На следующем слайде мы рассмотрим это немного подробнее. Опять же, это прямо из устава, поэтому я хотел бы повторить это. На ICANN возлагаются следующие обязанности. Во-первых, поддерживать связь по вопросам, касающимся работы корневых

серверов и их многочисленных экземпляров, с техническим сообществом Интернета и сообществом ICANN. RSSAC должен собирать и формулировать требования, чтобы предложить тем, кто занимается техническим пересмотром протоколов и лучших общих практик, связанных с работой DNS-серверов.

Во-вторых, общаться по вопросам, связанным с администрированием корневой зоны, с теми, кто непосредственно отвечает за это администрирование. Эти вопросы включают процессы и процедуры создания файла корневой зоны. В-третьих, постоянно проводить оценку угроз и анализ рисков для системы корневых серверов и рекомендовать любые необходимые аудиторские мероприятия для оценки текущего состояния корневых серверов и корневой зоны. В-четвертых, периодически отчитываться перед Правлением о своей деятельности, отвечать на запросы Правления о предоставлении информации или мнений, давать рекомендации по вопросам политики сообществу ICANN и Правлению.

В состав RSSAC входят члены с правом голоса, утвержденные операторами корневых серверов, и некоторые представители, не имеющие права голоса. Каждый из 12 операторов назначает основного и члена и его заместителя, и каждый оператор имеет в общей сложности один голос. В состав RSSAC входят представители без права голоса от Администрации адресного пространства Интернет, известной как IANA, от Администратора корневой зоны, более известного как RZM, от Совета по архитектуре Интернета, известного как IAB, и от Консультативного

комитета по безопасности и стабильности, или SSAC. Кроме того, RSSAC направляет своих представителей в Правление ICANN, Постоянный комитет потребителей (CSC), Комитет по обзору эволюции корневой зоны (RZERC), Номинационный комитет ICANN (NomCom), а также, по мере необходимости, в различные рабочие группы ICANN на специальной основе.

Кроме того, существует Группа подготовки RSSAC, которая представляет собой более широкую группу экспертов в данной области и включает в себя всех членов RSSAC. Членство в ней осуществляется по заявке, которая рассматривается Комитетом по членству Группы подготовки RSSAC. Требуются знания и опыт работы с инфраструктурой DNS, так как это группа экспертов, от которых ожидается выполнение значимой работы, а не место для изучения DNS. Существует список рассылки для членов, который позволяет получать приглашения на все заседания группы подготовки и список рассыли, но имеет более ограниченный вклад.

Важно понимать, как RSSAC разрабатывает политику. Этот процесс характеризуется структурированностью, открытостью и прозрачностью. Мы разрабатываем, выражаем и получаем отзывы о политике и планах, касающихся системы корневых серверов. По своей природе политика RSSAC рекомендуется для того, чтобы подтвердить давно установленную нормативную базу, используемую для работы системы корневого сервера, и предложить дальнейшее развитие, которое будет развиваться на основе этой существующей базы.

Важно понимать, чем RSSAC не является правоприменительным органом. RSSAC не является надзорным органом. RSSAC не является представителем операторов корневых серверов, и RSSAC не является представителем системы корневых серверов.

Как уже говорилось, RSSAC регулярно предоставляет письменные консультации по ряду тем, все они доступны на сайте ICANN. Здесь приведены примеры документов, которые дают представление о типе информации и рекомендаций, которые мы предоставляем. Они относятся к нескольким различным категориям. Например, история системы корневых серверов закреплена в документе RSSAC 002. В нем рассказывается о зарождении и развитии системы корневых серверов на протяжении десятилетий. Мы также публикуем руководство по оценке работы системы корневых серверов, которое можно посмотреть здесь.

Мы также приняли ряд рекомендаций, касающихся дальнейшего развития управления системой корневых серверов. Они также включают конкретные рекомендации Правлению ICANN по их исполнению.

На этом я завершаю свое введение в RSSAC, а теперь перейду к обсуждению DNS и роли, которую играет система корневых серверов в работе DNS. Чтобы было понятно, цель этой презентации - расширить ваше понимание системы корневых серверов и операторов корневых серверов. Мы объясним роль и назначение DNS, роль преобразователя адресов, роль авторитетного сервера, как, когда и почему преобразователь обращается к системе корневого сервера, а также

распространенные недоразумения, связанные с системой корневого сервера.

Теперь мы переходим к DNS, системе доменных имен. Мы расскажем о том, как работает DNS, что позволит нам представить систему корневых серверов, чтобы вы могли понять, как она вписывается в общий процесс. Представляем вам DNS. По своей сути DNS использует человеческие имена для поиска компьютерных адресов. Люди знают доменные имена; это просто, www.amazon.com. Компьютерам нужны IP-адреса. С ними сложнее, например 18.239.62.181. DNS - это способ, с помощью которого мы узнаем, что www.amazon.com действительно находтится по адресу 18.239.62.181.

В DNS номера могут меняться, а имена остаются неизменными. Поэтому подключенные устройства нуждаются в DNS, чтобы находить другие подключенные устройства. Изначально мы представляли себе это как ряд компьютеров и серверов; все большее число устройств - это смартфоны и смарт-устройства. В общем, вопросы DNS касаются доменных имен. Ответы даются в виде IP-адресов.

Преимущества DNS, очевидные и понятные всем, - это удобство для человека. Нам легче запомнить ряд слов, чем ряд цифр. Это несложно. Но, вероятно, не менее важно и то, что служба становится очень портативной. Вы можете присвоить доменное имя устройствам, к которым хотите привлечь людей, а затем менять адреса, где это необходимо. Вы можете изменить аппаратное обеспечение, платформу, местоположение,

топологию или почти все остальное. Потому что, пока у вас есть уникальное имя, DNS всегда приведет вас к новому онлайн-дому.

Это огромная распределенная сеть, которая удивительно проста в использовании. Она имеет гибкую делегированную базу данных, насчитывающую сотни миллионов каталогов, и, пожалуй, является крупнейшей в мире распределенной базой данных. DNS в двух словах. Разумеется, на практике все немного сложнее. Начнем с того, что устройства получают адреса от резолверов. В мире существуют миллионы резолверов, и резолверы, по сути, могут находить и читать то, что мы можем считать телефонными книгами интернета. Телефонные книги Интернета - это авторитетные серверы, которые хранятся у авторитетных людей, держащихся за свою часть Интернета. Эти списки похожи на телефонную книгу: содержимое зон, адресная информация и телефонные номера, которые вы найдете в телефонной книге.

Например, это сводится к тому, что вы задаете такой простой вопрос, как «Какой номер у www.amazon.com?», а ответ, когда я последний раз его искал, был 18.239.62.181. Это простой вопрос с простым ответом. Это происходит за миллисекунды. И это происходит, по нашим оценкам, 500 триллионов раз в день.

Резолверы получают свои адреса от авторитетных серверов. Помните, в прошлый раз мы говорили, что устройства получают информацию от резолверов, а резолверы - от авторитетных серверов. В большинстве случаев резолвер помнит, что обращался к авторитетному серверу, и помнит адрес для данного домена. Это называется кэшированием. Чаще всего ответ просто

хранится в памяти. Но иногда резолверу нужно узнать новый номер или подтвердить старый.

Итак, здесь мы пройдем через все слои DNS и узнаем, как это работает. В зависимости от того, сколько информации нужно резолверу, он либо не будет никого спрашивать. Он просто проверит свою собственную память, а она уже помнит ответ, полученный в последний раз, когда кто-то спрашивал его. Или, во втором случае, он обратится только к авторитетному серверу доменного имени. Мы ищем, допустим, www.example.com, и знаем, где находится example.com. Мы просто спросим их, где находится часть www?

В третьем случае мы потеряли больше информации, и знаем только, что она находится где-то в домене .com. Это домен верхнего уровня, .com. Затем мы спрашиваем у авторитетного сервера домена верхнего уровня, где находится это доменное имя? В четвертом случае, когда мы только что достали этот резолвер из коробки, или он только что проснулся, или его микросхемы только что сгорели от удара молнии, он должен знать все. Сначала ему нужно узнать, где я могу найти корневую серверную систему, чтобы найти авторитетный сервер TLD, чтобы найти сервер доменных имен, чтобы найти ответ. Поместите его обратно в кэш, и, надеюсь, мне не придется делать это снова.

Сейчас мы расскажем вам, как выглядит этот процесс внутри резолвера. Итак, слева находится серая рамка. Это и есть резолвер. Здесь у нас есть процесс, состоящий в основном из «да» и «нет», и мы собираемся посмотреть, как ответ начинается с

самого начала. Если вы видите слева вверху, задан вопрос, каков IP-адрес www.example.com? И то, что мы надеемся получить справа от него, и есть ответ. Вот ответ в виде адреса, возвращаемого входящему устройству.

Итак, в простейшем случае мы спрашиваем, каков IP-адрес www.example.com? Мы спрашиваем резолвера, знает ли он ответ на этот вопрос. В первом и самом распространенном случае резолвер отвечает: да, знаю. У меня есть эта информация, и я вам ее предоставлю. Итак, справа мы видим, что это происходит очень часто, и, по сути, это рутина. Именно так происходит более 90 % разрешений. Решателя спрашивают, есть ли у вас этот адрес? Он отвечает: да, есть. Он у меня в памяти.

Реже в памяти ничего нет. Итак, начинается вопрос: каков IP-адрес www.example.com? Резолверу задают вопрос: знаю ли я уже ответ? Резольвер отвечает: нет, я не знаю ответа. Тогда его спрашивают: ну, а вы, по крайней мере, знаете резолвер для example.com? И он знает. Тогда он говорит: отлично, авторитетный сервер example.com, помогите мне узнать, что такое www.example.com. Мы обращаемся к авторитетному серверу, который знает ответ. Он сообщает ответ. Мы помещаем его в память. Теперь мы спрашиваем, знаем ли мы ответ? Да, знаем, и мы даем ответ. Это простой одношаговый процесс.

Теперь предположим, что мы не знаем IP-адрес авторитетного сервера для example.com. Все, что мы знаем, - это example.com. Теперь мы спросим, каков IP-адрес www.example.com? Знаю ли я, специалист по разрешению, ответ? Нет, не знаю. Знаю ли я, где

найти его для example.com? Нет, не знаю. Могу ли я найти сервер, авторитетный сервер для всего, что находится в .com? Да, могу, и поэтому я спрошу его, что такое example.com? Авторитетный сервер .com отвечает: вот IP-адрес авторитетного сервера для example.com, и возвращает его в память. Знаю ли я ответ? Нет, потому что теперь мне придется вернуться и найти www. Сначала я нашел example.com. Теперь мне нужно найти www. Я должен создать эту штуку.

Я отправляю пример на авторитетный сервер. Он возвращает ответ. Я заношу его в память. Теперь я знаю ответ? Да, знаю, и опять же, все, что я сделал, - это вернул правильный IP-адрес для www.example.com, но, судя по тому, как мало знал резолвер, когда я впервые его спросил, ему придется пройти еще несколько шагов.

Итак, давайте впервые задействуем корневую серверную систему. Считается, что в одном случае из пяти или десяти тысяч резолвер знает так мало, что приходится спрашивать его вплоть до уровня корневой серверной системы. Итак, каков IP-адрес сайта www.example.com? Есть ли у меня ответ? Нет, его нет в памяти. Знаю ли я, как добраться до example.com, чтобы спросить? Я даже этого не знаю. Знаю ли я, как добраться до .com? Я даже этого не знаю. Я не знаю абсолютно ничего. Это базовый холодный резолвер.

Что он всегда знает, так это как найти корневые серверы. Итак, я отправляю им вопрос: как мне найти IP-адрес домена .com? Система корневых серверов, выполняя свою единственную задачу, передает адрес авторитетному серверу для TLD, доменов

верхнего уровня, и именно это делает ее корневым сервером. Мы сообщаем этот IP-адрес. Он попадает в память, и теперь машина может начать задавать эти гораздо более простые вопросы.

Знаю ли я адрес example.com? Нет, даже близко. Знаю ли я IP-адрес для .com? Да, вы только что узнали его из системы корневого сервера. Отлично, теперь я могу спросить у авторитетного сервера для .com, что он знает. Да, мы обратимся к нему, и он расскажет нам, как добраться до example.com. Мы возьмем этот адрес и занесем его в память. Я уже знаю весь ответ? Нет, мы знаем только два слова. Итак, знаю ли я авторитетный адрес сервера для example.com? Да, наконец-то, после всех этих шагов я его знаю. Я спрошу, как мне найти www.example.com? Авторитетный сервер знает ответ. Он дает мне IP-адрес. Мы заносим его в память, и теперь, когда я задаю вопрос, знаю ли я наконец ответ на вопрос, каков IP-адрес www.example.com? Ответ - да, и вот он.

Если вы поняли и смогли бы мне это пересказать, то можете получить хорошо оплачиваемую работу в качестве эксперта по DNS.

NICO CABALLERO: Единственное, Джефф, спасибо за очень подробное объяснение. Обычно это называется разрешением DNS, и, собственно говоря, в ICANN Learn есть очень хороший курс, который объясняет все это в более простой форме. Но я просто хотел добавить, Джефф, что весь этот кошмар различных шагов и всего остального в конце

концов сводится к кэшированию, которое составляет 90% DNS. Но вы продолжайте. Вы объясняете это гораздо лучше меня.

JEFF OSBORN: Главное, что следует запомнить из этого процесса, - почти в каждом случае все просто. По мере продвижения вниз по стопке они становятся все более маловероятными, а те, что сложнее, - все более и более маловероятными. В абсолютно нормальном случае все, что происходит, - это слишком много кликов, чтобы вернуться назад, но мы начинаем с поля, в котором написано: «Вы знаете ответ?» Ваша память говорит: «да», и вы получаете ответ. Подавляющее большинство случаев.

Вот более краткое описание. Есть три уровня вопросов, которые мы задаем. На первом мы спрашиваем о том, что мы знаем о доменном имени. Мы знаем example.com. Мы пытаемся найти то, что находится слева от него. Это www.example.com или mail.example.com или nameserver.example.com или что-то еще. Существует 350 миллионов мест, где это может быть, потому что в мире примерно 350 миллионов тех, что вы считаете доменными именами.

Доменные имена верхнего уровня - это гораздо меньшая группа. Если вам, например, нужно зайти на сайт .uk и спросить, что вы знаете о домене .uk, или что вы знаете о домене .edu, или что вы знаете о любом другом из этих доменов, то список будет гораздо меньше. В мире насчитывается около 1450 таких организаций, и в них, как правило, насчитывается от 1000 до 10 миллионов

объектов. Они полностью поддерживаются регистратурой доменов верхнего уровня. Поэтому люди, владеющие доменами .edu, .eu и .uk, несут полную ответственность за все эти имена.

Корневая зона, по большому счету, совсем крошечная. Это один документ. Это одна зона. По сути, это список из 1450 доменов верхнего уровня и адрес, по которому до них можно добраться. Вот и все. Он поддерживается не системой корневых серверов, а IANA, а затем криптографически закрывается группой под названием «Специалист по обслуживанию корневой зоны». Только после этого она становится общедоступной, и ее можно доставить и забрать из системы корневого сервера.

В обзоре корневой сервер хранит копию корневой зоны. Вот и все. Это вся информация, которая у нас есть. В корневой зоне хранятся адреса 1450 доменов верхнего уровня, которые вам известны. Мне нравится думать о них как о том, что находится справа от точки: .com, .nl, .jobs, .cz - целая куча всего.

TLD, каждый из этих TLD имеет авторитетный сервер, который знает адреса всех следующих шагов. Так что все имена, которые заканчиваются на .com, вы можете найти на авторитетном сервере .com и найти amazon.com, tiktok.com, freshflowers.com, asunnydayatthepark.com. Все они известны авторитетному серверу этого домена верхнего уровня. То же самое касается и других доменов, которые я включил в список: .nl для Нидерландов, .jobs как gTLD.

А когда вы дойдете до фактического доменного имени, например, jeffsgarden.org может быть организацией. Я тот, кто отвечает за все дополнения к доменному имени слева отсюда. Авторитетные серверы доменного имени контролируются владельцем регистрации, который является оператором доменного имени. Таким образом, существуют сотни миллионов авторитетных серверов для доменных имен.

Как видите, это иерархия. Резолвер просто находит и возвращает ответ. Мы грозились нарисовать это на футболке, поэтому я написал это крупным шрифтом. В миллисекундном мире резолвера запросы к корневой серверной системе редки. Это очень важный результат. Большинство вещей хранится в памяти, большинство вещей люди уже знают. Это редкий случай, когда вам приходится обращаться к корневой серверной системе, чтобы что-то найти.

Что касается системы корневого сервера, то она предоставляет информацию об адресе, а не о содержимом. Фактически, она предоставляет частичный адрес. Система корневого сервера буквально отвечает на одну небольшую часть вопроса об адресе. Все, о чем вы спрашиваете, все, о чем спрашивает резолвер у системы корневого сервера, это: «Можете ли вы дать мне адрес, где я могу посмотреть адреса доменов верхнего уровня?» Это часть адреса; это даже не весь адрес.

Это не контент. Система корневых серверов не размещает веб-контент, электронную почту или любой другой подобный интернет-контент. Она не доставляет его, не передает его, она не

имеет никакого отношения к контенту. Мы просто предоставляем небольшую часть адреса. Поэтому важно напомнить вам, что система корневых серверов не управляет интернет-контентом и не передает его.

Кроме того, система корневого сервера не является стражником в Интернете. Системы корневых серверов отвечают на запросы, задаваемые резолверами адресов, а резолверы адресов обычно строят свои ответы из кэш-памяти. Обычно им вообще не нужно спрашивать кого-то еще, но им приходится искать множество других мест, прежде чем они доберутся до корневого сервера, а когда они добираются до него, то только потому, что у них был действительно сложный вопрос и они находятся в очень забавном состоянии, только что выйдя из коробки или пережив удар молнии или что-то подобное.

В результате трафик почти всегда передается без необходимости ожидания на корневой серверной системе. По приблизительным оценкам, корневая серверная система возникает менее чем в одном случае из пяти или десяти тысяч.

Система корневых серверов удивительно стабильна, безопасна и устойчива по целому ряду причин. Во-первых, она обладает огромной избыточностью. В настоящее время существует чуть более 1800 глобально распределенных серверных экземпляров по всему миру. Каждый из них обладает 100% всей необходимой информации. Чтобы получить ответ, вам не обязательно иметь доступ к нескольким из них. Любой из них может предоставить вам адреса всех авторитетных серверов доменов верхнего уровня.

Мы работаем на различных аппаратных платформах. Существует огромное разнообразие используемого оборудования. Мы работаем на различных операционных системах. Мы используем множество приложений DNS поверх этих операционных систем, поверх этих аппаратных систем. И мы практикуем разнообразную маршрутизацию, так что в каждом случае информация поступает по-разному.

С точки зрения технологии это означает, что нет единой точки технологического сбоя. Ошибка Microsoft нанесет вред крошечной части нас. Ошибка практически во всем, что существует, нанесет вред крошечной части нас. Мы считаем, что очень важно признать, что разнообразие системы - это ее сила.

Аналогичным образом, система корневых серверов управляется 12 автономными операторами корневых серверов. Каждый оператор корневого сервера полностью независим от другого. Операторы корневых серверов постоянно сотрудничают с другими. Мы все, как правило, знаем друг друга. Мы часто разговариваем. Мы часто встречаемся. Но мы независимы. Мы независимы в том, как мы работаем, как мы собираем эти системы вместе и что мы делаем.

Очень важным результатом этого является то, что невозможно представить себе форс-мажорные обстоятельства, возникшие у одного оператора, например судебный запрет, как это, к сожалению, произошло с AFRINIC, который оказал бы операционное воздействие на всех остальных. Поэтому важно

признать, что в системе корневых серверов нет единой точки институционального сбоя.

Далее, стабильность, безопасность и отказоустойчивость - это то, о чем мы действительно много говорим. И это потому, что мы очень заботимся об этом. Мы внедряем их. Мы работаем над этим. И это правда. Система работает с 1980-х годов, и за все эти десятилетия не было ни одного случая отключения услуг. Это дольше, чем некоторые из вас живут.

DDoS-атакующие пытались это сделать и потерпели неудачу. Эта система специально создана удивительно устойчивой. В результате мы работаем уже более 30 лет, 7 дней в неделю, 24 часа в сутки, 365 дней в году. Я повторяюсь, но мне кажется, что это очень важно признать.

Это возвращает нас к тому, что мы не делаем. Операторы корневого сервера не решают, что находится в корневой зоне. Мы просто являемся надежным, аутентифицированным способом доставки. Регистрант, владелец доменного имени, определяет адресную информацию для своего домена. И он предоставляет адрес авторитетного сервера регистратуре TLD. Регистратура TLD определяет адрес своего авторитетного сервера и предоставляет его в IANA. IANA проверяет подлинность изменений адресов авторитетных серверов TLD и предоставляет их владельцу корневой зоны. Затем Специалист по обслуживанию корневой зоны криптографически подписывает корневую зону и предоставляет подписанную корневую зону операторам корневых серверов во всем мире.

Таким образом, эта информация поступает от пользователей через TLD, через IANA и в RZM. И к тому времени, когда мы ее получаем, она уже многократно подтверждена и криптографически подписана. Кроме нас, он находится в свободном доступе для всего мира. Если кто-то захочет проверить, совпадает ли полученный нами документ с тем, что есть у вас, это будет тривиально легко проверить.

В общем, система корневого сервера предоставляет адресную информацию TLD, а не Интернет-контент. Система корневого сервера не решает, какая информация TLD появляется в корневой зоне. Информация TLD предоставляется TLD, IANA и владельцем корневой зоны. Система корневого сервера не является стражником. Конечный пользователь имеет очень мало, если вообще имеет, прямых взаимодействий с конечными пользователями. Вероятность того, что кто-то из вас когда-либо сталкивался с задержкой в работе интернета из-за задержки, вызванной корневым сервером, практически равна нулю. Это крайне маловероятно.

В целом, система устойчива. В ней нет ни одной точки технологического сбоя. В ней нет ни одной точки институционального сбоя. И я очень благодарен вам за уделенное время.

NICO CABALLERO: Спасибо. Большое спасибо за очень подробную презентацию. Я знаю, что для вас это DNS 101, но нам нужно было изложить суть

для всего GAC. Опять же, на сайте ICANN Learn есть очень хороший учебник - на самом деле, я думаю, он называется DNS 101. Не уверен, но, вероятно, это тот самый случай. Я настоятельно рекомендую потратить, не знаю, может быть, 30 минут, не знаю, один час, чтобы понять... я не хочу, чтобы вы стали экспертами по DNS, инженерами-программистами, сетевыми инженерами или кем-то в этом роде, но это очень помогает понять нюансы, когда вы имеете дело с чем-либо, собственно говоря, с чем-либо, связанным с DNS, как, не знаю, криптография, например. Существует симметричная и асимметричная криптография. Мы можем говорить об этом часами, но пока спасибо вам еще раз, Джефф и Роб.

Есть ли у нас вопросы, комментарии или что-то, что вы хотели бы упомянуть в этот момент для Роба или для Джеффа? Давайте, пожалуйста, начинайте.

MARCO HOGEWONING: Спасибо, Джефф, за удивительно простую и понятную презентацию, и я надеюсь, что это - и никогда не бывает простого ответа, но я надеюсь, что у вас он есть. Как только что прошептал один из моих коллег, я уже почти никогда не набираю www, и действительно, если я скажу своему браузеру перейти на ICANN.org, он просто представит мне домашнюю страницу ICANN. Как это влияет на последовательность DNS-резолверов или на последовательность DNS-резолверов, которую вы только что объяснили?

JEFF OSBORN: Марко, это отличный вопрос. Важно помнить, что слова могут оставаться неизменными, а цифры меняться. Когда вы нажимаете на значок или щелкаете по подчеркиванию, он все равно использует слова доменного имени, чтобы сказать, куда он хочет попасть. Вашему приложению не нужно знать, что Amazon провела техническое обслуживание и переместила свой авторитетный сервер на другой адрес, потому что фраза, которую вы используете, все равно будет сопоставлена с правильным адресом. Они могут позаботиться о перемещении этих вещей в авторитетном бите.

Я объяснил эту презентацию своему сыну, которому 24 года, и он пытался сказать мне, сколько лет прошло с тех пор, как он набирал что-то в браузере. Так что у меня была та же самая дискуссия. Но, опять же, это возможность отображать ресурсы общим способом. Вы можете использовать что угодно, и это не обязательно должно быть понятным человеку. Просто должно быть известно, что если вы называете какую-то строку символов, то авторитетный сервер знает, как сопоставить ее с правильным адресом. Помогло ли это?

ROB CAROLINA: Я собираюсь сделать самую опасную вещь в мире, а именно, как юрист, попытаться объяснить что-то в DNS. Так что смотрите, как я упаду. Мои друзья меня поправят. Я считаю, что вопрос о том, разрешается ли что-то вроде ICANN.org на www.icann.org, также является вопросом, который настраивается владельцем

регистрации в зоне этого доменного имени. То есть это фактически функция DNS, которая может быть установлена и контролироваться владельцем регистрации. Некоторые владельцы регистраций предпочитают, чтобы их доменное имя по умолчанию всегда находилось в определенном месте. Другие оставляют его неопределенным, и тогда вы получаете ответ, в котором говорится: «Я не понимаю, о чем вы просите». Но в наши дни большинство коммерческих сайтов по умолчанию устанавливают www так, чтобы оно было невидимым или подразумевалось. Но это зависит от того, что решил владелец регистрации.

NICO CABALLERO: Спасибо, Роб. Спасибо, Нидерланды, за вопрос. У меня Папуа-Новая Гвинея.

RUSSELL WORUBA: Привет, председатель, и спасибо вам, наши уважаемые коллеги, за эту презентацию. Один наводящий вопрос по поводу доменов общего пользования верхнего уровня, которые будут представлены в этом раунде. Как корневые серверы распределяются в этой последовательности? Вписывается ли в нее появление нового домена общего пользования верхнего уровня? И если это вообще имеет значение, как это будет решаться?

JEFF OSBORN: Спасибо за вопрос. Новые домены верхнего уровня просто добавляются в файл зоны, и вместо 1450 доменов будет какое-то большее число. Что интересно, до 20 лет назад количество доменных серверов должно было увеличиваться по технологическим причинам, поскольку требовалось покрыть всю адресацию. Двадцать лет назад была внедрена интересная технология под названием Anycast, которая неожиданно значительно упростила надежную передачу очень больших объемов информации на очень большие территории.

И с тех пор корневой сервер не добавлялся, потому что мы поняли, насколько избыточны наши ресурсы. Точно так же, если мы удвоим или утроим размер файла корневой зоны, мы не увидим причин для изменения чего-либо, кроме буквального добавления имени файла корневой зоны. Если задуматься, документ с 1 400 строками текста - это не очень большой документ. Мы все каждый день делаем фотографии на свои телефоны, которые в тысячи раз больше этих. Так что переход от 1 400 к 3 000 или даже 4 000 или 5 000 должен практически не повлиять на работу системы корневого сервера. Помогает ли это?

RUSSELL WORUBA: Спасибо.

NICO CABALLERO: У меня есть Китай и США. Китай, вам слово, пожалуйста.

WANG LANG: Спасибо, Нико. Спасибо, Джефф, за подробную информацию. Как вы упомянули, существуют тысячи экземпляров системы корневых серверов, основанных на технологии Anycast и протоколах Border Gateway. Как вы думаете, могут ли эти экземпляры нести в себе больше рисков или угроз? Например, мошенничество или захват полномочий.

JEFF OSBORN: Существование мошенничества в корневых зонах - это то, с чем за 30 лет мы никогда не сталкивались, но, конечно, в мире безопасности вы всегда ищете сложное, необычное и редкое. Поэтому у меня возникает соблазн, поскольку передо мной сидят гораздо лучшие эксперты, чем я, и, возможно, кто-то из них сможет дать более подробный ответ. Поэтому, если вы не возражаете, я могу передать это моему коллеге из Швеции, Лиману.

LARS-JOHAN LIMAN: Спасибо. Извините, что я сижу спиной ко всем вам. Меня зовут Ларс-Йохан Лиман (Lars-Johan Liman). Я работаю в компании Netnod, операторе одного из кластеров корневых серверов. Проблема мошенничества - это то, что мы пытались решить, не мы, мы - все техническое сообщество в Интернете, не мы - операторы корневых серверов. Мы пытались решить эту проблему, добавив функции безопасности в данные DNS, функции DNSSEC, безопасные DNS, где все данные в корневой зоне и далее по дереву для тех, кто решит это сделать, но, конечно, в корневой зоне, все

данные криптографически подписаны, поэтому довольно легко проверить, что полученные данные верны.

Это делается на локальном уровне, в резолвере, который Джефф описал ранее, так что это может быть сделано очень близко к пользователю. Поэтому тот факт, что информация распространяется по многим экземплярам, не является большой проблемой благодаря DNSSEC. Можно проверить информацию на корректность, когда вы получаете ее очень близко к конечному пользователю. Спасибо.

NICO CABALLERO: Спасибо, Китай, за вопрос. Спасибо, Джефф, за подробный ответ. У меня есть США.

LEN HAWES: Доброе утро. Спасибо, Джефф. Я Лен Хоз (Len Hawes) из Государственного департамента Соединенных Штатов. Мой вопрос связан с избыточностью, о которой говорилось ранее, но у меня такой вопрос: существует ли постоянный процесс оценки, поскольку интернет-структура постоянно проверяет либо уровень использования, либо технологическое разнообразие этих точек на постоянной основе, чтобы убедиться, что у вас действительно диверсифицированная система?

JEFF OSBORN: Отличный вопрос. Спасибо, сэр. Интересная часть системы корневых серверов, как я уже сказал, заключается в том, что мы

действительно совершили небольшой скачок, когда разобрались с Anycast. И если вы хотите получить скучные, информативные 10 минут, поставьте меня в угол как-нибудь в коридоре, и я расскажу вам, как это работает. Но самое главное, что мы внезапно оказались перегружены и не в состоянии справиться с объемом. Большая часть интернета связана с попытками понять, как мы собираемся справиться с растущим объемом. Мы - одна из немногих организаций, где мы практически справились с этой задачей, поэтому мы стараемся обеспечить разнообразие, чтобы, если две компании купят друг друга, мы не оказались вдруг не разнообразными, потому что теперь мы оба используем их оборудование, чтобы при появлении развилок в операционной системе мы все были на достаточно разных системах.

Другая часть заключается в наличии достаточного количества устройств. В моей собственной организации, я являюсь президентом ISC, у нас есть несколько сотен инстанций, и наша программа позволяет, если вы сегодня написали мне письмо или спросили меня в коридоре, можем ли мы создать инстанцию у себя дома? В рамках некоторых довольно простых ограничений, он будет функционировать в течение, не знаю, в зависимости от тарифов, доставки и прочего, 30 дней, 60 дней.

Так что мы широко открыты, есть и другие организации, готовые, как и мы, просто добавлять новые экземпляры, когда это необходимо. Мы также тратим много времени на то, чтобы убедиться, что, опять же, трудно не быть техническим специалистом, но топология и география очень разные вещи, и

компьютерная топология часто означает, что вы можете посмотреть на географическую карту и почувствовать, что что-то не работает, в то время как топологически компьютеры на самом деле работают очень хорошо. Мы изучаем это довольно навязчиво. Поэтому мы уделяем этому много времени, и мы также очень открыты для любого мнения о том, как мы могли бы сделать это лучше.

ROB CAROLINA: Если говорить конкретно о вашем вопросе об обеспечении разнообразия, то операторы корневых серверов, помимо активного участия в RSSAC, также участвуют в других форумах, которые - в частности, один из форумов, не являющийся форумом ICANN, - посвящены операционным вопросам, связанным с системой корневых серверов. Обсуждения на нем не публикуются, поскольку они касаются очень важных оперативных деталей.

Отвечая на ваш конкретный вопрос, скажу, что эта группа активно изучает и исследует вопрос о разнообразии инфраструктуры среди операторов корневых серверов, потому что мы задавали себе те же вопросы на протяжении многих лет. И я могу, хотя мы не будем публиковать данные по понятным причинам, заверить вас, что мы очень рады обнаружить в результате наших внутренних опросов, что у нас именно такое разнообразие, которое Джефф описал ранее.

NICO CABALLERO: Спасибо, Роб, за ответ. У меня есть Европейская комиссия и джентльмен, который находится там. Говорите, пожалуйста.

ЕВРОПЕЙСКАЯ КОМИССИЯ: Спасибо. И спасибо за очень интересную презентацию. Я думаю, что она достигла своей цели - углубить понимание системы корневых серверов. Хочу сказать, что мы с большим интересом следим за работой RSSAC. Также мы понимаем, что вы работаете над обновлением структуры управления, и это отражается на многих консультативных документах, которые вы также недавно обновили. Хотелось бы узнать - и я понимаю, что это постоянный процесс - есть ли у вас какие-либо последние обновления или график того, как идет эта работа в настоящее время? Чем вы можете поделиться с нами? Спасибо.

JEFF OSBORN: При всем уважении, RSSAC - это не GWG. Есть организация, в которую входят некоторые члены RSSAC, но она не является RSSAC. Поэтому я не чувствую себя комфортно, выступая от имени отдельной организации в данный момент. То есть, я мог бы высказать свои личные соображения, наблюдая за происходящим со стороны, но я думаю, что это было бы безответственно по отношению к людям, которые на самом деле управляют и работают в GWG. Я точно знаю, что на этой неделе у нее будет несколько открытых встреч. Позже на этой неделе будет три или четыре или пять заседаний. Так что это открытые заседания; их легко проверить. Но при всем уважении, я не хочу говорить за GAC

и не хочу говорить за GWG, так что я прошу прощения. Я надеюсь, что не отвлекаю от темы; просто меня часто об этом спрашивают, и меня просили в этой организации: «Вы не говорите за нас, пожалуйста, не говорите».

ЕВРОПЕЙСКАЯ КОМИССИЯ: Позвольте мне, возможно, попытаться перефразировать. Мы просто пытаемся лучше понять роль RSSAC. В самом начале вы упомянули, что это не орган - не орган принуждения или надзора, не представительный орган для операторов услуг - и мы просто хотели понять это немного лучше, потому что я знаю, что вы работали над формализацией структуры управления. Вы упомянули об этом на нескольких слайдах в самом начале, просто пытаясь лучше понять, что вы можете рассказать о RSSAC, но не о других, конечно.

JEFF OSBORN: Хорошо, я передаю слово Робу.

ROBERT GOLDBERG: Это увлекательный процесс, над которым мы работаем. Роль RSSAC, или то, что RSSAC сделал как институт, имеет отношение к этому, - это основные предложения, которые RSSAC выдвинул, описывающие потребности структуры управления. Первоначальным документом, в котором это было сделано, конечно, был RSSAC-037, принятый несколько лет назад, в котором подробно описывались различные бизнес-процессы и различные

типы матрицы принятия решений, которые должны быть более формализованы по мере развития структуры управления системой корневых серверов. Это был путь и описание эволюции.

Аналогичным образом, RSSAC принял и опубликовал ряд основных нормативных принципов, которые формируют ключевую структуру управления, состоящую из 11 принципов, опубликованных в RSSAC 037 и повторенных и расширенных в RSSAC 055 несколько лет назад. Совсем недавно, в RSSAC 058, организация опубликовала очень длинный и подробный список критериев успеха - то, что, по нашему мнению, должно включать описание структуры управления, чтобы воплотить успех, чтобы двигать нас в правильном направлении. Этими рекомендациями RSSAC и, возможно, некоторыми другими, которые можно найти в опубликованных RSSAC документах, исчерпывается официальная роль RSSAC в текущих обсуждениях управления.

В рабочую группу по межсообщественному управлению, которая была создана Правлением, входят представители каждого из 12 операторов корневых серверов, а также других ключевых заинтересованных сторон в интернет-сообществе, сообществе ICANN, представители из различных источников. Таким образом, это другая комната, где люди обсуждают эволюцию, следующий шаг. И мы, говоря лично, очень положительно оцениваем направление, в котором движется процесс. И опять же, как и Джефф, я хотел бы обратиться к руководству GWG за более подробным отчетом. Однако я думаю, что это волнующая неделя

для GWG в позитивном смысле. Так что, надеюсь, это даст вам немного больше впечатлений.

NICO CABALLERO: Спасибо, Роб. Спасибо, Европейская комиссия, за вопрос. У меня есть последний вопрос, и я закрываю очередь, потому что у нас уже заканчивается время. Пожалуйста, продолжайте.

KHALED ALTARHUNI: Халед выступает, представитель Ливии в GAC. Спасибо, Джефф, за содержательную презентацию. Мне интересно, как работает система корневого сервера DNS, когда у нас есть два IP-адреса - IPv4 и IPv6 - для одного и того же домена? Используется ли при этом одна и та же база данных или...? Спасибо.

JEFF OSBORN: Короткий ответ: это работает очень хорошо. Это так называемый двойной стек, когда в DNS есть записи для IPv4-адресов и IPv6-адресов. Например, если вы буквально посмотрите на файл зоны - возможно, я единственный в этом зале, кто читает файлы зон, - но там есть, например, запись A - это запись для IPv4-адреса, а четверка A, то есть AAAA, - это запись для IPv6. И с тех пор как появился IPv6, системы по всему миру довольно хорошо умеют получать оба этих адреса. Все экземпляры корневых серверов на земле, которые я могу вспомнить, представляют запрашивающему и IPv4, и IPv6. Так что это полностью реализовано у нас. А мой

коллега из Швеции собирается усовершенствовать это, потому что он намного умнее меня.

LARS-JOHAN LIMAN: Спасибо. Снова Ларс-Йохан Лиман (Lars-Johan Liman) из компании Netnod. Нет, я не умнее вас, но я хотел бы добавить, что здесь есть два аспекта. Тот, который вы описали, - это содержимое базы данных, и ее содержимое - она содержит информацию как IPv4, так и IPv6. Но второй момент заключается в том, что все идентификаторы корневых серверов доступны через транспорт IPv6, так что если ваш компьютер использует только IPv6, вы все равно сможете добраться до корневых серверов. Не каждый из 1800, но я уверен, что более половины из них доступны, и на данный момент этого вполне достаточно. Спасибо.

KHALED ALTARHUNI: Спасибо.

NICO CABALLERO: Большое спасибо, Ливия, за вопрос. Я надеюсь, что вы получили ответ на ваш вопрос. И опять же, у нас совсем мало времени. Большое спасибо, Джефф, Роб, спасибо вашей фантастической команде. Аплодисменты нашим друзьям.

[КОНЕЦ СТЕНОГРАММЫ]