САН-ХУАН — ежедневное собрание стипендиатов
Понедельник, 12 марта 2018 года, 12:00 – 13:30 по AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Доброе утро! Конференция ICANN61, 12 марта, ежедневное собрание стипендиатов.

СИРАНУШ ВАРДАНЯН: Сегодня у нас особое собрание, его согласились провести для нас наши гуру в технических вопросах. У меня здесь прекрасная компания, и сначала я хочу предоставить слово Рейчел, а затем вы все остальные представитесь для стипендиатов, чтобы они знали, кто с каким докладом выступает.

Возьмите свои обеды, приходите и занимайте свои места, будьте внимательны. Это будет действительно очень интересное заседание, я уверена, вы не хотите его пропустить. Рейчел?

РЕЙЧЕЛ РЕЙЕС (RACHEL REYES): Здравствуйте. Добрый день! Добро пожаловать на заседание, посвященное основам DNS. Это заседание на полтора слота. В конце

презентации мы выделим минут 15-30 для ответов на ваши вопросы.

Меня зовут Рейчел Рейес. Я специалист службы технического обеспечения корпорации ICANN. Справа от меня сидит Джон Крейн (John Crain), который поможет мне в той части заседания, которая будет посвящена ответам на вопросы.

ДЖОН КРЕЙН: Я Джон Крейн. Я главный специалист ICANN по обеспечению безопасности, стабильности и отказоустойчивости. Я занимаюсь работой, связанной с эксплуатацией корневых серверов и других служб DNS, в течение последних 20 или 30 лет.

Там в углу на телефоне г-н Мэтт Ларсон (Matt Larson), которого также называют «Мистер DNS». Он также работал в отрасли DNS, наверное, еще дольше, чем я.

На этом я передаю слово назад Рейчел.

Рейчел Рейес: Хорошо, я надеюсь, мне удастся привлечь ваше внимание, даже когда вы едите. Итак, давайте начнем.

IP-адреса удобны для использования их в компьютерах, но справедливо также и то, что для нас проще запоминать имена, и сложнее — номера.

Возьмем, к примеру, кого-то из нас — по меньшей мере, для меня это так — очень трудно запомнить номера телефонов родственников или даже друзей, но зато они легко запоминаются по именам, и то же самое справедливо для запоминания имен или номеров в системе DNS.

В начале существования Интернета имена были простыми. Доменов тогда еще не было. Это однометочные имена из 24 символов, которые называются именами хостов.

Разрешение имен — это сопоставление IP-адресов и имен. В первые дни существования Интернета имена хостов хранились в файле HOST.TXT, это то, обновлением чего мы занимаемся, его обработка осуществляется централизованно сетевым информационным центром, или NIC, в Стэнфордском исследовательском институте. Они обновляют файл вручную, по электронной почте, новая версия выпускается раз в неделю, ее загружают по FTP. Так это было в самом начале существования Интернета.

Проблемой этой системы было то, что все изменения вносились вручную, то есть существовала большая вероятность ошибок, а эффективность работы была невысокой, потому что прежде чем вносить изменения, нужно было сначала разослать их по электронной почте. Кроме того, это требовало существенной полосы

пропускания, чтобы загружать и передавать этот файл. Так что это недолго просуществовало.

Именно поэтому в 1980-х начались разговоры о том, чтобы заменить существовавшую тогда систему. Была придумана концепция DNS, или системы доменных имен, которая позволила бы масштабировать работу существовавшей системы на основе файла HOST.TXT, а также упростить маршрутизацию электронной почты. В представленных здесь запроса комментариев (RFC) можно посмотреть другие документы, посвященные требованиям. В документах RFC 799 и RFC 819 изложена подробная информация о требованиях и о дискуссии, предшествовавшей созданию концепции DNS.

DNS в двух словах. Здесь мы обсудим сначала терминологию, которую мы используем в системе DNS. У нас есть DNS, данные DNS, резолверы, серверы имен, кэширование и репликация.

Я расскажу об этом подробно, используя этот график. У нас есть резолвер-заглушка, это еще один термин, о котором мы поговорим. И рекурсивный сервер имен, которые отправляет запросы к нашим серверам имен. То есть серверы имен — это те, которые для меня слева, а для вас справа. И вот эти серверы имен и дают точные ответы на запросы, которые присылает рекурсивный сервер. Здесь у нас маленькая подпись «кэш». Кэш используется в системе DNS для повышения ее

эффективности и масштабируемости. Чуть позже в нашей презентации мы рассмотрим это подробнее.

Пространство имен — это структура базы данных DNS в виде перевернутого дерева. Обычно древовидные структуры данных читаются сверху вниз, но в нашем мире DNS мы читаем их снизу вверх.

Возьмем, к примеру, этот график. Мы читаем это не как «.com.example.www». На самом деле мы читаем это как «www.example.com», это т.н. полностью определенные имена доменов.

В пространстве имен первым идет корень. Затем идут т. н. узлы верхнего уровня, потом узлы второго уровня, а после них — узлы третьего уровня.

У каждого из этих узлов есть своя метка. Эти метки состоят, или допустимыми символами для использования в метках являются только буквы, цифры и дефисы, все вместе — LDH.

Максимальная длина метки — 63 символа. Регистр при этом на самом деле не учитывается, так что можно писать и «com», и «cOm». На самом деле это не имеет значения.

У каждого узла есть свое доменное имя. В нашем примере мы используем это дерево. Выделенное здесь доменное имя — www.example.com. Его часть разделяются точками.

Как я уже сказала, полностью определенное имя домена, или FQDN, заканчивается точкой. Чаще всего, когда мы ищем доменное имя, мы на самом деле не используем точку в конце, а вводим просто «example.com» или «www.example.com».

Домен — это узел, и все, что ниже. В нашем примере верхним узлом нашего домена является .com, а все, что под ним — это территория зоны .com, или доменное имя .com.

Зоны — это административное деление, каждая зона DNS основывается на границах полномочий, которые делегируются какой-то организации. Та или иная зона DNS может состоять из одного или множества доменов или поддоменов. В результате делегирования образуются зоны. Делегирующая зона называется родительской, а создаваемая зона — дочерней.

Здесь родительская, т. е. корневая зона, делегировала информацию дочерним зонам .com, .uk и .coffee. А зона .com делегировала ее своей дочерней зоне, то есть .foo, .bar и пример.

Сервера имен, как я уже говорил — это сервера, отвечающие на запросы, которые поступают от рекурсивных серверов. Авторитативные серверы имен для той или иной зоны располагают полной информацией об этой зоне. По сути, когда отправляется запрос, если

рекурсивный сервер имен пустой, запрос направится непосредственно в зону, так нужно, поскольку там есть окончательная информация, касающаяся этого запроса. У зон есть несколько авторитативных серверов. Это делается для обеспечения избыточности и эффективности использования.

Как поддерживается синхронизация данных зоны между разными авторитативными серверами? У нас на самом деле есть этот протокол DNS, который встроен в сервер и который обеспечивает репликацию зоны. Это делается с помощью первичных и вторичных серверов.

Первичный сервер располагает окончательными данными зоны. Если нужно внести изменения в зону, это нужно делать на первичном сервере. С другой стороны, вторичный, или подчиненный сервер — это сервер, получающий данные зоны с другого авторитативного сервера. Этот процесс называется переносом зоны. Перенос зоны — это, по сути, обмен информацией между сервером DNS и другим авторитативным сервером.

Еще один сервер, который нам нужно здесь упомянуть, — это главный сервер, с которого и происходит файл зоны. Однако помните, что главный сервер не обязательно также первичный сервер. Вторичный сервер также может выступать в роли [главного] сервера.

Перенос зоны инициируется вторичным сервером. Это можно увидеть в этом стандарте, запросе комментариев RFC1996, в нем подробно описан процесс переноса зоны или внесения изменений в файл зоны.

Теперь мы переходим к ресурсным записям DNS. Ресурсные записи DNS — это то, что мы часто называем RR-записями. Если вы помните, я уже говорила, что у каждого узла есть свое доменное имя. У доменного имени есть другие связанные с ним данные, и эти данные доменных имен на самом деле хранятся в ресурсных записях.

Ресурсные записи бывают разных типов, но мы поговорим только о некоторых из них. Давайте перейдем к формату ресурсных записей. Ресурсная запись имеет пять полей: владелец, время существования, или TTL, класс, тип и RDATA. Владелец — это доменное имя, к которому относится данная ресурсная запись. Время существования — это время, на которое данная запись может кэшироваться сервером. Класс — это такой механизм расширяемости, обычно он не используется, поэтому чаще всего здесь указан класс IN. Тип — это тип данных, которые хранятся в ресурсной записи. A RDATA — это собственно данные, которые хранятся в ресурсной записи.

Я думаю, вам это более знакомо, если вы на это посмотрите, или я могу это вам показать. Эта

информация — это то, что называется ресурсными записями. Я думаю, большинство из вас, если вы знакомы с областью сетевых технологий, вам будет понятно то, о чем я говорила перед этим.

[Как здесь сказано], тип и RDATA всегда указываются, это обязательно. Вот чаще всего используемые типы ресурсных записей: Данные обозначают адрес протокола IPv4. AAAA означает IPv6. NS — это авторитативный сервер имен. SOA — это начало полномочий, они всегда отображаются на вершине зоны. В нашем предыдущем примере данные SOA находятся в домене .com. CNAME, или каноническое имя, — это псевдоним другого домена. MX означает сервер электронной почты (mail exchange). A PTR — это указатель, или это используется для обратного сопоставления.

Как я уже сказала, существует множество других типов ресурсных записей. По состоянию на декабрь 2017 года их уже 84. Чтобы получить более подробные сведения о таких типах ресурсных записей, вы можете перейти на этот сайт. Если вы перейдете на эту страницу, вы увидите вот это.

Давайте возьмем эти записи A и AAAA. Как я уже сказала, запись A выглядит так. Это вам даст адрес IPv4, а запись AAAA даст вам адрес IPv6.

Сервер имен, он помечен NS, он указывает авторитативный сервер имен для зоны. Он отображается в двух местах, родительский и дочерний. В данном примере с левой стороны зона имени, а с правой стороны сервер имен, а не IP-адрес.

Таким образом запись сервера имен обозначает делегирование от родительского сервера дочернему. В домене .com есть 13 серверов имен. По сути, это 13 корневых зон. Это показано здесь, от корня и аж до домена .com.

Во время делегирования мы включаем также связующую запись. Что такое связующая запись? Связующая запись — ресурсная запись протокола IPv4 или IPv6. В рамках делегирования она включается в родительскую запись. Эта связующая запись нужна нам потому, что, если, скажем, подать запрос IP-адреса для имени www.example.com, вы попадете прямо в корневую зону. Корень выдаст вам IP-адрес сервера имен. Затем вы спросите уже у сервера имен: «Какой IP-адрес у сайта www.example.com?». И так получится закольцованный цикл до тех пор, пока вы не сможете найти ответ на свой вопрос, потому что IP-адреса еще нет. Вот поэтому нам нужна связующая запись.

Записи SOA расположены в вершине зоны. Вот пример того, как выглядит запись SOA. Здесь есть ваш домен, ваш сервер имен. Администратор зоны

hostmaster.example.com. И серийный номер — это текущая версия файла.

Обновление означает время в секундах, которое вторичный сервер имен должен ждать, прежде чем проверять наличие изменений. Повтор попытки означает время в секундах, которое вторичный сервер имен должен ждать, прежде чем повторять перенос зоны после неудачной попытки. Срок годности означает время в секундах, которое вторичный сервер имен может использовать данные, прежде чем обновлять их, или же они становятся недействительными. И минимум — это TTL, время существования.

Запись CNAME, или каноническое имя, создает псевдоним для обращения к одному домену из другого. Справа от меня, для вас, наверное, слева, указана запись CNAME, а затем, справа, каноническое имя и домен, на который указывает псевдоним. Помните, что запись CNAME создает псевдоним и указывает на каноническое имя, но нужно помнить о том, что этим нельзя злоупотреблять. Не создавайте цепочки или петли. Кроме того, это не пойдет данным на пользу.

Тип записи MX, mail exchange. MX означает сервер электронной почты и предпочтение для доставки почты. В нашем примере сказано example.com MX 10 mail.example.com. Соответствующие числа, 10 и 20, это порядок маршрутизации или приоритетность

маршрутизации электронной почты. Чем меньше это значение, тем лучше. Это наш предпочтительный способ [неразборчиво] маршрутизации электронной почты.

Обратное сопоставление. Чаще всего нам нужно узнать IP-адрес для заданного доменного имени, однако иногда мы ищем пространство имен, а не IP-адрес. В таких случаях очень полезны ресурсные записи PTR. Они не всегда используются, однако со стороны сети в данных они всегда есть. Вот так это выглядит.

Позвольте мне спросить Джона Крейна, почему у нас здесь in-addr.arpa.

ДЖОН КРЕЙН: in-addr.arpa, как мы это называем, — это реверсирование адресов. Некоторые протоколы на самом деле проверяют это, чтобы гарантировать сопоставление имени и номера в обе стороны.

РЕЙЧЕЛ РЕЙЕС: Хорошо, итак, это другие типы ресурсных записей, которые у нас есть, но мне они на самом деле редко попадаются на глаза, разве что CDS и CDNSKEY, которые входят в DNSSEC.

Это пример файла зоны для домена example.com. У него есть SOA, сервер имен, IPv6, IPv4, запись MX, а также CNAME. А в последней части связующая запись. Так что

он уже указывает IP-адрес, как я уже говорила. Без этого он бы просто зацикливался.

Теперь переходим к процессу разрешения имен. Как я уже сказала, у нас есть резолверы-заглушки, рекурсивные серверы имен и авторитативные серверы имен. Эти серверы совместными усилиями выполняют поиск данных DNS в пространстве имен.

Резолверы-заглушки являются локальными для клиента. Они могут работать в вашем телефоне или ноутбуке. Затем рекурсивные серверы имен, опять же, они направляют запросы к авторитативному серверу имен. Авторитативные серверы имен отправляют ответы на такие запросы.

Запрос DNS всегда состоит из трех параметров, а именно: доменного имени, класса и типа, это то, что у нас есть в этом примере.

Два вида запросов. Резолверы-заглушки отправляют рекурсивные запросы, а затем рекурсивные серверы имен отправляют нерекурсивные или итеративные запросы, которые еще называются обращениями. Мы обсудим это позже.

Пожалуй, я это пропущу.

Это мне нужно обсудить, потому что если, скажем, вы начинаете процесс разрешения имени, в котором

рекурсивный сервер не указан или только что подключился. У вас тогда не будет других вариантов, кроме обращения прямо к корневым серверам имен, потому что на них расположены файлы корневой зоны.

Как какой-либо сервер имен находит корневой сервер имен? Они должны быть настроены. Это настраивается администратором сервера, обнаружить их нельзя.

Это список корневых серверов имен и файл с подсказками корневой зоны. NS — это серверы имен. A — это IP-адрес IPv4. AAAA — это IPv6.

Администрирование корневой зоны — это очень сложная тема, мы не будем ее обсуждать. Нам нужно быть проще. Если вы хотите узнать об этом больше, предложите Мэтту Ларсону арахисовые M&M, он выделит время и расскажет вам об этом. Но мы здесь об этом говорить не будем.

Есть две организации, которые сотрудничают в администрировании содержания корневой зоны, по сути, это ICANN и Verisign. Есть еще 12 организаций, поддерживающих работу авторитативных серверов имен. Возможно, вы спросите, почему 12, если на самом деле у нас 13 корневых серверов. Это потому, что у Verisign их два: сервер A и сервер J. Почему их у них два? Опять же, вам смогут ответить на это Джон Крейн и Мэтт Ларсон, однако, наверное, они не будут об этом говорить здесь.

Наверное, не на этом заседании, разве что Джон уделит минутку и расскажет нам эту историю?

ДЖОН КРЕЙН: Нет. Просто так сложилось исторически. В последний раз серверы имен распределялись в 90-е, когда добавлялись новые серверы имен, не все из них достались новым организациям, а два из них не нашли себе дома. Один из них отправился на восточное побережье США в компанию Verisign, у которой были прочные отношения с Джоном Постелом и ISA, а другой остался в ISA, это был сервер L. Когда была сформирована ICANN, этот сервер отошел ICANN, а J, конечно же, остался у Verisign. То есть они просто так исторически были распределены.

РЕЙЧЕЛ РЕЙЕС: Ну вот. Если вы хотите знать, какие корневые серверы расположены в какой стране, вы можете перейти на этот веб-сайт: root-servers.org. Я на самом деле могу его вам показать. Допустим, вы ищете доступные серверы имен в Пуэрто-Рико. В настоящее время в Пуэрто-Рико доступны серверы L и J. Так что если вы хотите ознакомиться с этой информацией, можете зайти на этот веб-сайт.

Кроме того, у нас есть Anycast-зеркала этих корневых серверов, благодаря чему можно найти ближайший к вам DNS-сервер или корневые серверы в вашем регионе. Это

также помогает при поиске. Это работает эффективнее, если есть экземпляры недалеко от вас.

Процесс изменения корневой зоны. Как сказано на этом слайде, это упрощенная версия. На самом деле за всем этим стоят еще другие процессы. Мы не будем о них говорить, мы просто в общих чертах рассказываем вам о том, как меняется файл корневой зоны.

По сути, все начинается с того, что менеджер TLD передает изменение в IANA. Затем IANA выполняет этот запрос, внося для этого сначала изменения в базу данных корневой зоны, а затем создавая файл корневой зоны и публикуя корневую зону на всех корневых серверах.

Теперь переходим к процессу разрешения имен. Когда вы делаете запрос со своего телефона, на самом деле происходит следующее. Не обязательно только с телефона. Это может быть ноутбук или какой-нибудь другой клиент. Каждый клиент — ноутбук, телефон — оснащен резолвером-заглушкой, это локальный резолвер клиента.

Затем он задает вопрос: «Какой IP-адрес у сайта www.example.com?». Этот вопрос направляется вашему рекурсивному серверу с IP-адресом 4.2.2.2, это запрос «Какой IP-адрес у сайта www.example.com?». Ваш рекурсивный сервер имен отвечает что-то вроде

следующего: «Я не знаю, но, возможно, эта информация есть у корневого сервера».

А у вашего рекурсивного сервера имен этой информации еще нет потому, что это совершенно новый рекурсивный сервер имен. Как уже было сказано, незаполненный или новый рекурсивный сервер имен еще не располагает всей информацией из кэша, поэтому он обращается непосредственно к корневому серверу и запрашивает у него IP-адрес, потому что на корневом сервере есть файл корневой зоны.

Затем ваш корневой сервер возвращает ответ: «Я не знаю этот адрес, но я знаю адрес домена .com». Поэтому ваш рекурсивный сервер имен обращается к серверам домена .com и спрашивает: «Какой IP-адрес у сайта www.example.com?». Затем ваш сервер имен домена .com отвечает: «Я не знаю, но я знаю IP-адрес сервера имен и ns1.example.com».

Так что теперь ваш рекурсивный сервер обратится к этому серверу по адресу ns1.example.com, и этот сервер имен выдаст IP-адрес или даст точный ответ на ваш запрос. Затем ваш рекурсивный сервер имен вернет IP-адрес вашему резолверу-заглушке.

Это все выполняется считанные секунды. Это занимает не минуты. Это получается похоже на то, как вы запускаете приложение на телефоне или на ноутбуке.

Иногда загрузка страницы или запуск приложения занимает какое-то время. Но когда вы пробуете загрузить страницу еще раз, это происходит уже гораздо быстрее. Почему? Потому что необходимая информация уже сохранена в кэше вашего клиента.

Давайте еще раз. Кэширование ускоряет процесс разрешения имен, потому что теперь имя и IP-адрес вашей корневой зоны и ваших серверов имен уже известны. Если вы попытаетесь обратиться к ним или подать запрос: «Какой IP-адрес ftp.example.com?», — а недавно мы спрашивали IP-адрес сайта www.example.com.

Теперь мы запрашиваем IP-адрес сайта ftp.example.com. Так что ваш браузер или резолвер-заглушка еще раз обратится к рекурсивному серверу имен, но в этот раз он уже не будет обращаться к корневой зоне, а перейдет непосредственно к серверу имен, потому что эта информация уже сохранена в кэше. Кэширование позволяет ускорить этот процесс и сделать его эффективнее. Вот так работает процесс разрешения имен.

У нас здесь есть слайд о DNSSEC на одну страничку. Если вы хотите получить более глубокие знания о DNSSEC, для этого есть несколько заседаний. У нас есть на этой неделе заседание, посвященное DNSSEC, которое они могли бы посетить?

ДЖОН КРЕЙН: Я посмотрю, но на самом деле у нас будет скоро заседание по DNSSEC. Кажется, в среду, но я еще посмотрю до конца нашего заседания.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Вчера был учебный семинар.

РЕЙЧЕЛ РЕЙЕС: Что ж, превосходно. Итак, по сути, это основы DNSSEC. Я просто прочитаю это вам. Посредством DNSSEC данные DNS можно защитить с помощью цифровой подписи, удостоверяющей их подлинность. У каждой зоны есть своя пара из закрытого и открытого ключей для работы с DNSSEC.

Несколько записей в DNSSEC — это DNSKEY, то есть открытый ключ зоны, RRSIG, или цифровая подпись. NSEC или NSEC3 — это указатель на следующее имя в зоне, а DS — это подписант делегирования.

Еще раз — если вы хотите получить более подробную информацию о DNSSEC, вы можете посетить одно из заседаний, посвященных DNSSEC, которые проходят на этой конференции.

Экосистема доменных имен работает следующим образом. У нас есть регистратура, у которой есть база

данных доменных имен и их владельцев, потом у нас есть регистратор, который является основным посредником между владельцами доменов и регистратурой, а владелец домена — это держатель зарегистрированного доменного имени.

Это процесс работы регистратуры доменных имен, но мы не будем обсуждать весь этот процесс. Я просто пытаюсь вам сказать, что то, о чем мы только что говорили, — это часть всей регистратуры доменных имен. Мы обсудили то, что здесь, где авторитативный сервер имен, рекурсивный сервер имен и пользователь Интернета.

Это все, что у меня есть для сегодняшнего заседания, возможно, у кого-то есть вопросы.

ДЖОН КРЕЙН: Прежде чем мы перейдем к вопросам, я хочу дать информацию по DNSSEC. Это будет в среду, с 9:00 по 15:00, это будет целый день, посвященный DNSSEC. Больше, чем кому бы то ни было может понадобиться.

РЕЙЧЕЛ РЕЙЕС: Хорошо.

СИРАНУШ ВАРДАНЯН: Да, мы можем переходить к ответам на вопросы. Да, пожалуйста.

НИКОЛАС ФЬЮМАРЕЛЛИ (NICOLAS FIUMARELLI): Здравствуйте. Николас Фьюмарелли из Уругвая. Вы сказали, что DNS не различает регистр символов, а как обстоит дело с интернационализированными доменными именами?

РЕЙЧЕЛ РЕЙЕС: На этот вопрос может ответить Мэтт.

МЭТТ ЛАРСОН: Сама по себе DNS точно не различает регистр. Интернационализированные доменные имена — это своего рода надстройка над DNS. Я попрошу вас, Рейчел, вернитесь, пожалуйста, назад, к одному из слайдов, посвященных пространству имен, в самом начале. Пожалуйста, продолжайте. Хорошо. Спасибо.

Если вы посмотрите на этот слайд, я хочу сказать, этот узел в верхней левой части, который начинается с xn--, то, как мы решили поступить с интернационализированными доменными именами, как я уже сказал, мы решили реализовать их в виде такого слоя-надстройки.

С точки зрения пользователя, если приложение поддерживает интернационализированные доменные имена, пользователь при взаимодействии с таким приложением видит доменные имена в написании

символами соответствующего языка. Однако затем это приложение должно преобразовать такие символы в формат LDH, то есть буква, цифра, дефис — это тот формат, который понимает DNS.

Так что с точки зрения DNS они выглядят так же, как и обычные метки, только немного смешно. Вы можете видеть эти символы «xn--» — это код, что остальная часть этой метки представляет собой закодированное интернационализированное доменное имя. На самом деле существует специальная кодировка, которая называется Punycode, это своего рода игра слов, обыгрывающая название Unicode, она создана специально для того, чтобы кодировать символы Unicode для меток в DNS.

НИКОЛАС ФЬЮМАРЕЛЛИ: Спасибо.

МЭТТ ЛАРСОН: Да. Просто чтобы вы немного представили себе предысторию, когда мы над этим работали, были и те, кто спрашивал: «А зачем нам нужна эта надстройка над DNS? Почему бы нам просто не реализовать, скажем, UTF-8 прямо в DNS? Давайте предусмотрим метки в DNS в кодировке UTF-8».

Были вполне понятные опасения в отношении того, что система DNS может быть к этому не готова, потому что она не для этого создавалась. Так что нам пришлось бы модернизировать всю инфраструктуру DNS, и нам все равно пришлось бы обновлять все клиенты для поддержки кодировки UTF-8 в метках.

Поэтому при реализации интернационализированных доменных имен мы исходили из таких соображений: «Да, нам все равно придется обновлять все клиенты, однако по крайней мере нам не придется менять все остальное в инфраструктуре DNS». То есть вопрос был в том, как много нам придется всего менять. Хотите ли вы менять все, приложения и инфраструктуру DNS, или же только приложения?

СИРАНУШ ВАРДАНЯН: Ладно. У нас здесь вопрос. Прошу вас.

АБДУЛКАРИМ ОЛОЙЕДЕ (ABDULKARIM OLOYEDE): Спасибо. Я хочу прежде всего задать вопрос к тому, что вы сказали. Вы сказали, что это надстройка над DNS. В то же время, если я правильно это понял, это значит, что если вы отправляете запрос на DNS-сервер, вы отправляете его весь на DNS-сервер. То есть как это у вас получается эта надстройка над DNS? Это вопрос к тому, что вы сказали, прежде чем я задам свой вопрос.

МЭТТ ЛАРСОН: Разумеется. Когда я говорю, что это надстройка над DNS, я имею в виду, что концептуально это оно и есть, но на самом деле это реализовано в приложениях, поддерживающих интернационализированные доменные имена.

Например, в современном веб-браузере, поддерживающем интернационализированные доменные имена, вы вводите какие-то символы из нелатинского алфавита, а он преобразовывает их в некую метку, начинающуюся на xn--. Это может быть xn--., xn--нечто. То есть это интернационализировано на уровне метки. А затем веб-браузер отправляет запрос, вызывает резолвер-заглушку, а резолвер-заглушка отправляет этот запрос на сервер имен, и в этом запросе метки записаны в формате xn--.

То есть когда я говорю, что это надстройка над DNS, я имею в виду, что это реализовано в приложении, а не на серверах и резолверах DNS.

АБДУЛКАРИМ ОЛОЙЕДЕ: Спасибо. Теперь я перейду к моему вопросу. У меня два вопроса. Первый из них такой: когда вы проводили свою презентацию, я не знаю. Может, я что-то пропустил, когда я ел, или вы говорили слишком быстро. Что касается серверов зоны. Вы сказали, что это

довольно сложно. Я не совсем понял о серверах зоны. Что вы имеете в виду, когда говорите о серверах зоны? В особенности когда вы говорите о первичных серверах зоны, вторичных серверах зоны, а потом вы говорили, что эти серверы зоны бывают главными и подчиненными. Вы не могли бы еще раз объяснить эту часть?

А другая часть моего вопроса касается адреса 4.2.2.2 — он используется, когда вы отправляете любой вопрос, или это как рекурсивный сервер для всех запросов по умолчанию?

ДЖОН КРЕЙН: Если вы имеете в виду разные типы серверов имен, мы обычно не называем их серверами зоны, то существует, по сути, три типа таких серверов. Есть заглушка, которая реализована в вашем ноутбуке или в вашем телефоне, к примеру, она также может быть реализована в операционной системе или собственно в приложении, например, в браузере. Они только отвечают на вопросы.

Затем бывают рекурсивные серверы, которые обычно работают у вашего интернет-провайдера, или же они могут быть реализованы в маршрутизаторе у вас дома. Они, если можно так сказать, передают запросы дальше. Эти серверы обращаются к авторитативным серверам. Это те серверы, у которых есть ответы на запросы. Поэтому они и называются авторитативными, то есть

уполномоченными. У них есть полномочия давать ответы. Именно на них, то есть на авторитативных серверах, расположены файлы зоны.

На рекурсивных серверах есть механизм запросов, который перенаправляет запросы. На них данные хранятся только в кэше. То есть это как память, которая запоминает ответы. Это может быть и на вашем резолвере-заглушке. То есть существует маршрут передачи запросов от вашего устройства и дальше по иерархии.

Там, кстати, был еще один комментарий, кажется, его сделала Рейчел, о том, как сложно устроена работа корневой зоны. Я не знаю, имели ли вы в виду это. Это совсем другое. Там целая система выделения ресурсов, это не то же самое, что и система серверов имен. Пусть об этом расскажет Мэтт, если захочет, потому что он работал над некоторыми аспектами этой системы с другой стороны.

А какой рекурсивный сервер будете использовать вы, обычно определяется при настройке вашего компьютера или вашей сети. Когда вы подключаетесь посредством какой-либо сети, например, здесь, мы используем протокол динамической конфигурации узлов, то есть DHCP. Именно он направляет вам те IP-адреса, которые вы используете, но он может также присылать вам ваши доменные имена и ваши рекурсивные серверы. Этих у вас

может быть два. Этих у вас может быть один. Этих у вас может быть четыре. И тогда все запросы от вас направляются на настроенные у вас серверы.

СИРАНУШ ВАРДАНЯН: Есть вопрос от удаленного участника. Хорошо, закончите этот.

МЭТТ ЛАРСОН: Вы спросили конкретно об адресе 4.2.2.2. Это сервер, работу которого поддерживает интернет-провайдер Level 3 Communications. Это т. н. открытый рекурсивный сервер. Обычно, если где-то есть много клиентов — то есть это может быть любая сеть, это может быть интернет-провайдер для своих широкополосных клиентов или сеть ICANN в этом здании — если где-то есть много клиентов с резолверами-заглушками (см. внизу слева), то в верхней части должен быть рекурсивный сервер.

Как сказал Джон, за предоставление такого рекурсивного сервера отвечает оператор сети, а когда вы подключаетесь к сети, ваше устройство получает от этого рекурсивного сервера IP-адрес, чтобы настроить свою конфигурацию.

При этом вы не обязаны использовать этот рекурсивный сервер. Вы можете использовать другие. Существуют разные очень популярные рекурсивные серверы, то есть

принимающие запросы от всех. Их можно назвать независимыми рекурсивными серверами или общедоступными рекурсивными серверами. Пожалуй, самый популярный из них, потому что его адрес так легко запомнить, — это открытый DNS-сервер Google по адресу 8.8.8.8. Так что при желании вы можете настроить на своем телефоне резолвер-заглушку. Вы можете изменить конфигурацию на адрес 8.8.8.8 вместо того, который вам дает ваш интернет-провайдер.

Есть еще другие популярные серверы, Open DNS уже давно работает. Они были одними из первых, кто решил вынести рекурсивные серверы за пределы сетей и предоставлять такие услуги. У Verisign такие есть. У PCH есть то, что они называют Qaud9, то есть четыре девятки, 9.9.9.9. Так что таких общедоступных серверов есть несколько, и 4.2.2.2 от Level 3 тоже уже очень давно работает.

СИРАНУШ ВАРДАНЯН: Спасибо. Есть вопрос от удаленного участника [неразборчиво] из Африки. «Африка, по всей видимости, постепенно развивается, и есть необходимость в наращивании потенциала. Программа стипендий позволяет сократить разрыв в возможностях представителей развивающихся стран, однако помимо этого, что намерена делать ICANN или, если говорить об

этом, DNSSEC, для наращивания потенциала? И что нам нужно делать в Африке в том, что касается политик?».

ДЖОН КРЕЙН: Наращивание потенциала, мы говорим о DNS, так что я буду говорить о потенциале в том, что касается DNS. Мы обычно работаем с сообществом. Моя группа, в частности, мы проводим множество учебных мероприятий для развития потенциала. Однако в Африке, в частности, чаще можно видеть такие организации, как AfriNIC, или, если взять AFNOG и AfTLD (это домен верхнего уровня AF), чаще можно видеть, как такое обучение проводят эти организации. А мы работаем с ними и поддерживаем их.

Есть еще одна организация, которая называется Центр ресурсов для запуска сетей, она очень активно работает в Африке в сфере обучения по вопросам DNS и другим проблемам, связанным с инфраструктурой.

Если говорить конкретно о DNSSEC, мы провели в африканском регионе множество учебных мероприятий совместно с AFNOG и, по сути, со всеми африканскими доменами, со всеми африканскими организациями, которые там есть. Я не помню, на когда запланировано следующее такое мероприятие, однако, думаю, несколько практических занятий, посвященных DNSSEC, должно быть запланировано для Африки на май-июнь.

То есть мы на самом деле очень активно там работаем, но мы полагаемся на местных специалистов. Если вы хотите научить чему-то наш мир, а он очень большой, то это не задача ICANN. ICANN — это, конечно, небольшая организация. Некоторые все равно считают, что она слишком большая, но, тем не менее, это небольшая организация. Поэтому на самом деле мы связываемся с местными сообществами технических специалистов и помогаем им, мы либо даем им материалы, либо работаем вместе с ними на основе их материалов. Такой подход работает лучше, чем многие другие.

Мы также работаем на некоторых образовательных онлайн-платформах, которые позволят нам использовать потенциал электронных средств обучения, а также упростят задачи по переводу материалов на различные языки.

Так что несмотря на то, что нас нельзя назвать всемирным университетом, мы на самом деле уделяем много времени тому, чтобы учить людей. Один из моментов, если вы посмотрите на название моей должности, там есть слова «безопасность, стабильность и отказоустойчивость», мы беспокоимся об экосистеме. А чтобы как-то усовершенствовать положение дел в этой области, один из способов — дать людям более удобный доступ к знаниям и способность создавать более совершенные системы.

СИРАНУШ ВАРДАНЯН: Спасибо. Лендон?

ЛЕНДОН ТЕЛЕСФОРД (LENDON TELESFORD): Здравствуйте. Я Лендон Телесфорд из Канады. Я не уверен, касается ли этот вопрос DNS как таковой или всей системы в целом. Я не уверен, возможно ли это, но я все равно спрошу. В презентации были выделены зеркала Anycast и различные экземпляры корневых серверов. Мой вопрос звучит так: какие механизмы реализованы в этой схеме клиент-сервер и Anycast для защиты от атак DDoS, которые воздействуют на определение расстояния до серверов, когда клиенты не могут точно определить, к какому серверу обращаться?

ДЖОН КРЕЙН: Я пытаюсь обдумать этот вопрос. Хотите ответить?

МЭТТ ЛАРСОН: Я не совсем понимаю, что вы имеете в виду, когда говорите, что клиенты не могут точно определить, к какому серверу обращаться. Я хочу в своем ответе еще раз использовать эту концепцию слоя, надстройки. Anycast — это на самом деле слой уровнем ниже DNS. У нас есть DNS, а Anycast относится к системе маршрутизации в Интернете.

Давайте возьмем систему корневых серверов, в которой, я думаю, на данный момент абсолютно каждый IP-адрес является Anycast. Допустим, у нас есть рекурсивный сервер имен, который собирается отправить запрос корневому серверу L. На уровне слоя DNS он просто говорит: «Отправляю запрос на следующий IP-адрес».

Однако когда этот запрос попадает на уровень маршрутизации, когда соответствующий пакет должен быть передан собственно сетью, маршрутизаторы в сети будут видеть, что на самом деле существует несколько экземпляров, несколько разных мест в сети, в которых присутствует данный IP-адрес. Что касается того, как это выглядит с точки зрения динамического протокола маршрутизации BGP, можно сказать, что разные сети объявляют маршрут к нужной сети. То есть несколько сетей в Интернете заявляют: «Я могу передать на корневой сервер L». «Я могу передать на корневой сервер L». «Я могу передать на корневой сервер L».

Отдельные маршрутизаторы используют эту информацию протокола BGP при принятии собственного решения. «Какой с моей точки зрения оптимальный маршрут к корневому серверу L?». Это делают все маршрутизаторы. Это означает, что, когда вы говорите «Мне нужно направить пакет на корневой сервер L», то, в зависимости от того, где именно в сети вы находитесь, вы направляетесь к ближайшему к вам экземпляру. При этом

учитывается не только географическое расстояние. Не только задержки. На политику маршрутизации протокола BGP влияют самые разные факторы.

Я не совсем понимаю, как сюда приписать то, о чем вы говорите, что они не могут определить расстояние. Может произойти так, что, в случае атаки на один экземпляр этот экземпляр может быть перегружен, а операторы обычно настраивают Anycast-конфигурацию серверов имен таким образом, что, когда сервер имен работает, он как бы говорит сети: «Я здесь. Я существую, так что можете объявлять маршрут на меня». Однако если перегрузка настолько велика, что он не сможет продолжать работу, это зависит от того, как именно произойдет отказ, в удачном случае такой сервер скажет сети: «Все, меня больше нет. Я не могу принимать запросы DNS». Тогда сеть перерассчитает маршруты и будет направлять трафик куда-то еще.

ЛЕНДОН ТЕЛЕСФОРД: То есть на стороне маршрутизатора решения о направлении маршрутизации принимаются на основе заранее заданной информации протокола BGP?

МЭТТ ЛАРСОН: Я бы не сказал, что она заранее задана. Она все время меняется. Каждая сеть, каждый номер автономной системы, как мы их называем, то есть это сеть с точки

зрения протокола BGP, а автономная система — это сеть, у которой есть какой-то набор маршрутов, объявляемых ею сетей, о которых она говорит: «У меня есть вот эти IP-адреса».

То есть каждый маршрутизатор, использующий протокол BGP, постоянно говорит: «Мне известны следующие сети», а другие маршрутизаторы принимают это к сведению и в режиме реального времени принимают решения о том, что где находится. Это очень, очень упрощенная картина того, как это все работает, но протокол BGP — это информация, которая постоянно меняется в режиме реального времени.

ДЖОН КРЕЙН: Я хочу добавить, что это не обязательно из-за Anycast. Это было еще до Anycast, потому что к тому или иному узлу может быть несколько разных маршрутов. Если кто-то объявляет сайт, возможно, если я нахожусь действительно далеко, я увижу только один маршрут, но если он расположен относительно близко, к нему может существовать несколько маршрутов. И то же самое было и раньше. То есть это такая особенность маршрутизации, которая известна и используется для добавления серверов. Для Anycast технология не менялась. Это просто такой прием маршрутизации.

ЛЕНДОН ТЕЛЕСФОРД: Я просто хотел спросить, можно ли как-то обмануть эту особенность маршрутизации.

ДЖОН КРЕЙН: Не думаю, что это касается этого приема. С маршрутизацией могут быть связаны свои проблемы в области безопасности, но это проблемы, связанные с маршрутизацией, а не с технологией рассылки пакетов Anycast. У маршрутизации действительно есть свои проблемы с безопасностью или, возможно, правильнее сказать, недостаточно проблем с безопасностью. Но они не специфичны для Anycast.

СИРАНУШ ВАРДАНЯН: Спасибо. Вон там, прошу вас.

ШАБНИЛ АНАЛ САМИ (SHABNIL ANAL SAMI): Здравствуйте. Это Шабнил с Фиджи. У меня такой вопрос: если какая-то страна захочет разместить у себя корневой сервер, как с практической точки зрения лучше всего решить, какой именно сервер выбрать? Ну, то есть из этих 13 — A, L, F или какой-то еще? Или это зависит от региона? Или кто-угодно может разместить у себя сервер?

ДЖОН КРЕЙН: Это зависит от того, с кем вы решите поговорить. Начнем с того, что это не страна делает, я бы сказал. Разместить у себя экземпляр сервера может сеть или сетевой оператор. Он может перейти на сайт root-servers.org и посмотреть список операторов. Один из этих операторов — мы. Кажется, у нас уже есть один сервер на Фиджи, думаю, еще кто-то это делает.

Вы можете просто связаться с этими операторами и спросить их о том, какие условия они выдвигают для этого. Они могут немного отличаться у разных операторов, но это несложно. На сегодняшний день существует 990 экземпляров таких серверов в разных местах. Так что чтобы добавить еще несколько, нужно просто связаться с кем-то. Перейдите на веб-сайт root-servers.org, там на самом деле есть ссылки на каждого оператора, вы можете ознакомиться с их документацией и узнать, как с ими связаться. Они будут рады пообщаться с вами онлайн и рассказать вам, как это сделать.

ШАБНИЛ АНАЛ САМИ: Мне просто интересно, какой именно выбрать, то есть L, F. Что, просто перейти? Потому что я вижу, что в Пуэрто-Рико размещен сервер L, на Фиджи размещен сервер L, то есть я просто не понимаю эти региональные аспекты. Спасибо.

ДЖОН КРЕЙН: Да, это не вопрос региона. Это зачастую вопрос отношений. На Фиджи размещен корневой сервер L, который стал там уже вторым, потому что у нас есть представитель персонала на Фиджи, Саве Восеа (Save Vocea). Так что очень часто это зависит от того, с кем у вас налажены отношения или с кем вы выстраиваете отношения, когда вы заходите на сайт и говорите: «О, этот ничего так».

Кроме того, у разных операторов могут отличаться критерии, в первую очередь финансовые критерии. К примеру, у нас в ICANN есть решение, в рамках которого вы оплачиваете сервер, подключаете его к Интернету, а затем всю работу делаем мы. Кто-то другой пришлет вам сервер, если вы дадите ему денег. Эти модели может немного отличаться, так что вам нужно выяснить, какая из них вам больше подходит.

С точки зрения DNS все корневые серверы равны. Все они дают одни и те же ответы. То есть с точки зрения ответов на запросы они все работают одинаково. Так что вопрос на самом деле в том, с кем вам удобно выстраивать рабочие отношения, или, возможно, с кем вы знакомы.

ШАБНИЛ АНАЛ САМИ: Хорошо, спасибо.

СИРАНУШ ВАРДАНЯН: Другие вопросы? Да, пожалуйста.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: У меня два вопроса. Как может быть обеспечена правильность [дупликации] областей из регистратур стран, чтобы не [выбирались] неправильные [неразборчиво], как это произошло много лет назад? Второй вопрос — являются ли копии корневых серверов, которые размещены в разных странах, к примеру, только частью [неразборчиво] по всему миру, только частью [неразборчиво] этого корня. К примеру, корневой сервер L имеет только часть всех [неразборчиво] или же у него есть все записи?

МЭТТ ЛАРСОН: Нет, все корневые серверы располагают одинаковой информацией. Есть только одна корневая зона и соответствующая ей информация, и на каждом корневом сервере эта информация одна и та же.

Не могли бы вы повторить свой первый вопрос?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Например, когда регистратура [неразборчиво].

СИРАНУШ ВАРДАНЯН: Просто вопрос: у нас есть перевод. Вы можете сказать это на своем языке.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Хорошо.

МЭТТ ЛАРСОН: Отлично. Отлично.

СИРАНУШ ВАРДАНЯН: Так что воспользуйтесь этой возможностью.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Что ж, хорошо. Одну секундочку, пожалуйста.

СИРАНУШ ВАРДАНЯН: Да. Подождите минутку, чтобы все успели надеть наушники.

НЕНАЗВАВШАЯСЯ ЖЕНЩИНА: Проверка. Вы слышите перевод на английский? Вы слышите английский? Что ж, превосходно. Спасибо.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: [через переводчика] Когда записи в каждой стране, есть записи в зоне, например, ccTLD, если у регистратуры есть запись в зоне, она публикуется и распространяется через зоны DNS, как можно гарантировать, что эти публикуемые записи являются правильными, что не было никаких ошибок при публикации или распространении таких зон? Потому что, если я правильно понимаю, в прошлом такое уже бывало.

ДЖОН КРЕЙН: Здесь на самом деле несколько вопросов. Я отвечу за то, что касается терминологии и технологии. Итак, независимо от того, ccTLD это или gTLD, когда они публикуют зону, эта зона состоит из данных, происходящих из их собственных баз данных, и они несут ответственность за обеспечение достоверности этих данных. Когда они уже опубликованы, если зона подписывается с помощью DNSSEC, а запросы DNS проходят проверку подлинности, тогда можно гарантировать, что вы получите то, что было опубликовано.

И это все. Это то, что касается опубликования данных и DNS. А все остальные аспекты этого на самом деле относятся к области безопасности сетей, а также безопасности баз данных и целостности ваших данных. В прошлом имели место проблемы, когда хакеры проникали в системы ccTLD, я думаю, вы об этом.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Да.

ДЖОН КРЕЙН: Не бывает стопроцентной безопасности сетей. На каком-то уровне, я думаю, люди всегда будут подвержены таким угрозам. Мы в ICANN и наши друзья в этих регистратурах, в частности, моя группа, группа по безопасности, мы делаем следующее — когда они сталкиваются с проблемами, они обращаются к нам, а мы помогаем им с восстановлением. Мы часто также помогаем им в поиске специалистов для переработки их систем.

У нас было несколько проблем в прошлом и я думаю, что знаю, какую из них вы имеете в виду, но я не хочу называть. В нескольких случаях имели место атаки типа внедрения SQL. Это конкретная атака на системы оператора.

Тогда злоумышленники получили возможность изменить записи крупной организации и перенаправлять браузеры пользователей на другие адреса. То есть это выглядело — если я говорю о том случае, а я думаю, что говорю о том случае, который вы имеете в виду — для внешнего наблюдателя это выглядит так, как будто веб-сервер был взломан. Но на самом деле это не так. Это были системы регистратуры.

То есть в том случае мы много работали с этим оператором регистратуры, и сейчас у него реализована совершенно новая система, которая прошла аудит и защищена от этого. Они извлекли опыт из своих ошибок и пошли дальше, это то, что мы делаем, когда сталкиваемся с проблемами безопасности. Вы понимаете, что у вас проблемы с безопасностью, вы исправляете недостатки своих систем, учитесь на своих ошибках и совершенствуете свои процессы.

Но это не означает, что никакой другой ccTLD или даже gTLD где-нибудь еще вообще никогда не будет взломан, потому что так просто не бывает. Мы видим, как атакам подвергаются крупнейшие корпорации, которые тратят на это миллионы долларов.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Большое спасибо.

СИРАНУШ ВАРДАНЯН: Да, пожалуйста.

ДЖЕЙСОН ХАЙНДС (JASON HYNDS): Джон, я хочу спросить об этом.

СИРАНУШ ВАРДАНЯН: Как вас зовут?

ДЖЕЙСОН ХАЙНДС: О, извините. Да. Я Джейсон Хайндс с Барбадоса. Джон, у меня вопрос к тому, что вы сказали — есть ли какие-то ваши публикации, которые могли бы помочь операторам регистратуры в предотвращении таких распространенных видов атак?

ДЖОН КРЕЙН: Работая с некоторыми нашими партнерами, о которых я уже говорил, когда речь шла о наращивании потенциала, мы провели для операторов тысячи часов обучения по таким вопросам, как обеспечение безопасности сетей, ведение мониторинга сетей. Разумеется, сообщество операторов, представителей которого вы видите здесь, также имеет свои группы и также делится какими-то передовыми практическими методиками и оказывает друг другу помощь, в том числе техническую помощь.

К примеру, на Ямайке, которая относится к региону LAC, есть такая организация LACTLD, объединяющая все регистратуры этого региона... не все, но большинство из них. Они проводят регулярные встречи и технические совещания. Когда одна из них сталкивается с проблемами, другие приходят ей на помощь.

То есть это не та проблема, с которой они остаются наедине. Это проблема, затрагивающая все сообщество.

Она решается сообща, через обучение и взаимопомощь, там много всего.

СИРАНУШ ВАРДАНЯН: Вопросы? Больше вопросов нет.

Я бы рекомендовала вам непременно принять участие в этом семинаре по DNSSEC, который пройдет в среду с 9:00 утра и до обеда.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: До 3:00.

СИРАНУШ ВАРДАНЯН: До 3:00.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Это долго.

СИРАНУШ ВАРДАНЯН: Хорошо, тогда в середине мы проведем рабочий обед для стипендиатов. Но в любом случае, прошу вас, приходите на наш семинар. Это действительно очень важно.

Какие-то заключительные слова от наших докладчиков?

РЕЙЧЕЛ РЕЙЕС: Спасибо вам всем за то, что вы были сегодня с нами. Я благодарна вам за ваше участие. Спасибо, Джон и Мэтт, за то, что помогали мне отвечать на вопросы.

СИРАНУШ ВАРДАНЯН: Я хочу поблагодарить наших переводчиков и специалистов службы технического обеспечения. Огромная благодарность от меня вам, Мэтт, Джон и Рейчел, за то, что вы уделили нам свое время. Я знаю, что вы очень заняты во время этой конференции, поэтому спасибо, что пришли и провели эти презентации для наших стипендиатов. Ваши аплодисменты нашим выступавшим.

На этом объявляю наше заседание закрытым. Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]