ICANN79 | CF – Знакомство с сообществом ICANN: мероприятие по налаживанию деловых связей для членов SSAC и RSSAC
Воскресенье, 3 марта 2024 г. – 4:30 – 5:30 по SJU

СИРАНУШ ВАРДАНЯН (SIRANUSH VARDANYAN): Большое спасибо. Итак, это наша последняя на сегодня встреча с участниками программ Fellowship и NextGen, на которой мы поговорим об аспектах безопасности и стабильности ICANN, и мне очень приятен интерес, проявленный со стороны RSSAC, Консультативного комитета системы корневых серверов, и SSAC, Консультативного комитета по безопасности и стабильности. Они пришли к нам, и мы имеем удовольствие общаться с ними в такой обстановке, почти тет-а-тет. У нас будет 30 минут в начале для выступления представителя RSSAC, затем 30 минут для выступления SSAC, 5-10 минут презентаций, а затем ответы на вопросы.

Рам, пожалуйста, присоединяйтесь к нам. Итак, первым выступит председатель RSSAC Джефф, он расскажет и объяснит, чем занимается это сообщество, насколько оно важно, и каким образом новички могут принять участие в его работе. Большое спасибо. Вам слово, Джефф.

ДЖЕФФ ОСБОРН (JEFF OSBORN): Здравствуйте! Вы меня слышите? Это первая часть взаимодействия с аудиторией. Самая легкая. Дальше

будет сложнее. Меня зовут Джефф Осборн. Я председатель RSSAC — организации при ICANN, которая консультирует по вопросам, связанным с системой корневых серверов DNS. И нам поручено попытаться простыми словами объяснить, чем мы занимаемся. А потом я услышал, что мне предстоит выступить перед вами, ребята. И мы потратили кучу времени на создание этой презентации, чтобы попытаться объяснить людям, которые не занимаются DNS с утра до вечера, что такое DNS и как работает система корневых серверов. В конце презентации вы станете экспертами. У вас появится новая страница в резюме. Вы сможете сразу же, возможно, уже завтра, получить гораздо лучшую работу. Но придется слушать внимательно, потому что это сложновато.

Итак, сегодня мы работаем с презентацией, которую составили три дня назад. В ней есть пара незначительных моментов, которые я собираюсь просмотреть, потому что, как я уже сказал, вижу это в первый раз. Мы узнаем, как работает DNS, какова роль системы корневых серверов в DNS, и узнаем, насколько важна система корневых серверов. Консультативный комитет по корневым серверам состоит из людей, которые управляют корневыми серверами. Есть 12 организаций, управляющих корневыми серверами. Есть один член и один его заместитель, два раза по 12 равно... вы, ребята, хорошо в этом разбираетесь. Вы получите эту работу. 24. Кроме того, у нас есть представители в нескольких других структурах, таких как Правление ICANN и — вы, наверное, уже об этом слышали, — Инженерная проектная группа Интернета, Совет по архитектуре Интернета, ряд технических организаций.

Так что мы стараемся привлекать специалистов отовсюду, откуда только можно.

Позвольте мне рассказать вам о DNS. Сначала ICANN. Одна из первых вещей, на которые я обратил внимание в ICANN, почему это слово не пишется просто I-C-A-N? Произношение одинаковое. В ICANN недаром две буквы N. Первая N — это имена, вторая — IP-адреса. Запомнить длинную строку цифр сложнее, чем запомнить слово. Поэтому DNS использует имена для поиска адресов компьютеров. Сами компьютеры понятия не имеют, что такое amazon.com. Все, что они понимают, это строка из букв. Итак, люди знают доменное имя amazon.com. Я хочу туда зайти. Компьютер ожидает услышать 18.239.62.181, что буквально является сегодняшним IP-адресом Amazon.

И DNS это переводит. Вы вводите это в браузер. Система DNS это переводит, и по большей части вы можете использовать одно и то же имя, независимо от того, что меняется в фоновом режиме. Адреса могут быть в разных местах, в разных странах, на разных серверах, но вы всегда используете только имя. Это очень удобная система, и в основе ее лежит система доменных имен. Когда люди говорят о DNS, речь идет об использовании слов, чтобы добраться до цифр. Кому-нибудь нужно, чтобы я повторил еще раз, или это понятно? Слова для поиска номеров. Прекрасно.

СИРАНУШ ВАРДАНЯН: Одобряем.

ДЖЕФФ ОСБОРН: Одобряем. Хорошо. Итак, большинство подключенных устройств используют DNS, чтобы добраться до чего-либо в интернете, а интернет, как вы, наверное, слышали, большой. Так что это сложно, и вот как мы это делаем. Конечно, есть такие вещи, как компьютеры и серверы, которые используют для подключения, но все чаще пользователями становятся сотовые телефоны, и, не приведи господь, стиральные машины, холодильники, дверные звонки и прочее. Мы все используем DNS, чтобы ориентироваться в интернете. Преимущества этой системы в том, что вам просто нужно запомнить имя. Если ваш компьютер сломается и вы купите новый, его все равно можно будет называть Jeff'sComputerHut.com. Неважно, сменил ли я сервер, переехал на другую улицу или у меня сгорел дом. Так обеспечивается мобильность сервисов.

Это очень важно с точки зрения того, чтобы не зацикливаться на одном поставщике. Вы не будете привязаны к одному интернет-провайдеру. Вы даже не будете привязаны к одной стране. Люди, у которых есть доменное имя, могут этим пользоваться, как и еще одной внутренней фишкой ICANN. Вы не собственник доменного имени, если оно у вас есть. Вы — владелец домена. Кто из присутствующих здесь является владельцем домена и не знал об этом? И это тоже можно указать в своем резюме. Так и напишите: «Я — владелец домена». Гарантирую, что в большинстве мест это добавит еще 10 % к зарплате. Это малоизвестный секрет, совет

профессионала. Но все же главное преимущество DNS — это простой идентификатор человека. Меня проще узнать, если я jeff@isc.org, нежели jeff@118.36.12.92. А я помню время, когда приходилось заниматься подобной ерундой. Так что эта система лучше.

СИРАНУШ ВАРДАНЯН: Джефф, если можно говорить помедленнее, для переводчиков, это было бы здорово. Спасибо.

ДЖЕФФ ОСБОРН: Существует ли противоядие от кофе? Я постараюсь помедленнее.

СИРАНУШ ВАРДАНЯН: Спасибо.

ДЖЕФФ ОСБОРН: Это сложно. Мне нравится говорить быстро. Я постараюсь помедленнее. Устройства получают эти адреса от того, что вы называете резолвером. Вы наверняка слышали термин «резолвер». Во всем мире их миллионы. Знакомый вам 8.8.8.8 — это резолвер, который компания Google разместила повсюду. Если вы направите на него свое устройство, оно скажет вам, где что находится. Их миллионы и миллионы. В основном они действуют так, как будто читают телефонные книги. Идея заключается в том, что телефонная книга — это так называемый авторитативный

сервер, а цифры в ней — это данные зоны. И когда вы запрашиваете там www.amazon.com, они наводят справку и выдают адрес. Все занимает миллисекунды. Это невероятно быстро и происходит ошеломляющее количество раз.

По нашим оценкам, в среднем за день это происходит 500 триллионов раз. 500 триллионов — это очень много. Если вы сейчас начнете считать до 500 триллионов, то никогда не закончите. Это огромное число. Сами резолверы получают адреса от так называемого авторитативного сервера. Итак, начнем с того, как эти вещи соединяются в сети, кто с кем общается и откуда все это берется. Резолверы постоянно получают запросы, как добраться до Amazon?

В их памяти хранится адрес, чтобы не искать каждый раз. Поэтому, если вы зададите им простые вопросы, например, где находится amazon.com, где находится tinder.com, где находятся эти вещи, они просто выдают вам ответ из своей памяти. Это называется кэшированием. Они хранят их в так называемом кэше. Именно оттуда приходит большинство ответов. Когда вы запрашиваете информацию о том, как что-то найти, в 90% случаев ответы приходят именно оттуда, из памяти.

Время от времени вам нужно получить новый номер или подтвердить старый, и ему приходится отправляться на сервер и искать его. Внимание, переходим к технической части. Существует трехуровневый процесс, через который он должен пройти. В зависимости от того, сколько информации вам нужно узнать об

этом адресе, вы либо обратитесь к авторитативному серверу доменных имен, либо к авторитативному серверу доменных имен и серверу доменов верхнего уровня.

Домен верхнего уровня — это домены .com, .uk, .nl и т.п. Или сервер доменных имен, сервер доменов верхнего уровня и корневой сервер, в зависимости от того, чего ваш компьютер не знает. Итак, посмотрим на схему. Эта схема — либо лучшее, что можно было придумать, чтобы понять, как это работает, либо она настолько запутанная, что вы скажете: зачем здесь все эти буквы? Ничего не понять. Так что слушайте меня. Попытаемся в этом разобраться.

Во-первых, вот здесь вверху. Вы можете прочитать эти буквы? Хорошо. Сперва серый квадрат — это резолвер, и мы задаем ему вопрос. Мы начинаем извне и говорим: мне нужен адрес www.amazon.com. Знаю ли я, где он находится? Нажимаем. И резолвер отвечает: да, знаю. Он у меня в памяти. Вот, пожалуйста. Вот адрес. И вот мы снова идем в конец. И справа, вы видите, написано, что это стандартная процедура. Так происходит в более чем 90 случаев из 100. В 90% случаев вы просто получаете данные из памяти. Но адресов многие сотни миллионов адресов, и иногда вы их не знаете. Что если я не знаю ответа? Первый вопрос, который вы зададите: знаю ли я, где находится сервер, который может знать ответ?

В таком случае вы отправите запрос: мне нужно узнать IP-адрес для www.example.com. В итоге мы получаем авторитативный сервер, потому что у example.com есть собственное место для

поиска всех букв. Что стоит перед example.com? Это может быть www. Это может быть почта. Это может быть целый ряд вещей. Мы спрашиваем его, и он выдает адрес. Мы запомнили его и теперь спрашиваем, знаем ли мы уже ответ? Да, знаем. Итак, мы рассмотрели два простых случая. Знаю ли я ответ? Да, он в памяти. Или знаю ли я ответ? Нет, но я знаю, где находится сервер, который знает ответ. Он сообщает его мне, теперь я храню его в памяти и сообщаю ему.

Единственное, что усложняет ситуацию, это сотни и сотни миллионов устройств, и все они не могут уместиться на одной машине, поэтому здесь целых три уровня. Так что, если у вас нет возможности добраться до example.com, придется спуститься еще на шаг ниже и подумать, а не выбрать ли example.com вместо www.example.com? Это отдельный сервер. Он называется сервером TLD. Если вы получаете от него информацию, он скажет: мы знаем, где это. Мы знаем, где мы сейчас находимся? Нет, вы только что выяснили, где находится example.com. Нам нужно вернуться и добавить www, и теперь мы знаем оба этих адреса. Эта схема включает три шага, и как только вы дойдете до третьего шага — все готово. Если вы это поймете и будете соблюдать, то так DNS и работает.

Если вы не знаете абсолютно ничего, если ваш компьютер только что достали из коробки, у него нет памяти и он ничего не знает, одну вещь он все-таки знает. Внизу, в левом нижнем углу, он знает адреса корневых серверов. Это мы. Есть 12 адресов для 12

операторов корневых серверов, и вы можете найти один из них и спросить: а где список для .com? Я ничего не знаю. Мне просто нужно знать, что находится справа от точки? Я ищу .com, потом спрошу, где находится example, а потом спрошу, где находится www. Вы получаете ответ, запоминаете его, возвращаетесь и ищете example, возвращаетесь и ищете www. Вы создали имя, найдя все адреса. Вы сохранили его в памяти. Вот и все. Теперь вы все эксперты в области DNS. Это будет в вашем резюме. Мои поздравления. Плату за обучение можете оставить у двери. Мы принимаем наличные, чаевые.

Самое интересное — это частота. Если вы видите красные буквы сбоку: количество случаев, когда это происходит из памяти, составляет более 90%. Количество случаев, когда вам приходится спускаться ниже и — о, черт, я даже не знаю, что такое example.com, — составляет еще около 5%. Приходится выходить и спрашивать, где находится .com и что он знает? Это около 2%. Пройти весь путь до корня, до корневого сервера — это примерно одна попытка из 5000. Мы действительно важны, если вы все забыли, но далеко не каждый раз, когда вы что-то делаете, вы должны попасть на корневой сервер. Мы ваш запасной вариант. Понимаете? Должна ли это быть футболка? Я думал об этом. Это может быть слишком сложно для чтения. На подходе еще один слайд с футболкой, так что мы с этим разберемся.

В общем, корневой сервер хранит копию данных корневой зоны, а корневая зона рассказывает вам о том, что есть в доменах

верхнего уровня. Вы просто хотите знать: расскажите мне обо всем, что заканчивается на .com. Расскажите мне обо всем, что заканчивается на .uk. Расскажите мне обо всем, что заканчивается на .nl, и он выдаст вам все это. Он выдаст вам одно слово слева. Авторитативный сервер TLD, второй шаг вниз, знает все адреса для следующего шага. После того как вы получили Amazon и .com, он знает www, и знает почту, и знает DNS-сервер, и знает возвраты, и знает «джон точка что угодно». Все остальное на той стороне. Резолвер — это устройство, которое работает и знает, как объединить эти три процесса и предоставить вам необходимую информацию, чтобы у вас был адрес того места, куда вы пытаетесь попасть.

В мире, где все происходит за миллисекунды, запросы к корневым серверам редки. Мы постоянно сталкиваемся с этим: поскольку корневой сервер абсолютно необходим, если вы все забыли, люди думают, что абсолютно необходим каждый шаг, а это не так. Это действительно важная и нужная вещь, но по большому счету вы не всегда работаете через корневой сервер. Когда ваша бабушка ищет рецепт печенья, корневой сервер не задействован. Он задействован очень редко, и некоторые утверждают, что это один случай из 10 000. Это как минимум один случай из 5000. Просто это не происходит часто. Понимаете?

Этот слайд мы убрали сегодня утром, он понравился Раму, и мы случайно поставили его обратно, так что это довольно забавно. У меня будут неприятности, если я покажу эти цифры, потому что

они сказали, что мы не можем это доказать, но мы уверены, что тут все верно. Вполне возможно, что число запросов в день составляет около 500 триллионов с буквой T. Это шокирующее число. Это невероятно много, но представьте все случаи, когда на вашем компьютере появляется URL, и ему нужно что-то выяснить, и каждый человек на земле делает это. Вот примерно такое число. На корневые серверы, мы полагаем, поступает около 100 миллиардов вопросов в день, что тоже очень много, но это всего один из 5000 в общем количестве. Так что речь об очень больших цифрах, и именно этим мы и занимаемся.

Важно помнить, что объем большой, а частота — нет. Что мы делаем, чтобы этот ценный ресурс всегда работал? Несколько вещей. Во-первых, он многократно резервируется. Каждый корневой сервер содержит всю информацию. Если вы перейдете, например, на .com, он должен помнить 140 миллионов вещей, которые нужно поместить слева от .com. Корневые серверы должны помнить только 1700 TLD. В настоящее время существует только 1700 слов справа от точки, от .com до .edu, до NL, до всех национальных доменов, всех коммерческих доменов. Их 1700. В текстовом виде это не очень обширная информация. Оказывается, каждый из этих корневых серверов сам по себе может обслуживать большую часть потребностей Земли. У нас их 1700. Если у вас есть два компьютера двойного назначения для резервирования, и один из них умирает, то второй продолжает работать.

По состоянию на прошлый месяц, я думаю, их было 1758 по всему миру, и 1757 из них даже не особо нужны. Представьте ситуацию: вы теряете такое количество, а все это все равно работает. Это поразительно устойчивая система. У нас разные аппаратные платформы. Все используют разные компьютеры для работы. Мы используем разные операционные системы. У всех разные операционные системы. Мы используем разные приложения DNS. На своей основной работе я — президент компании ISC, и, помимо управления сервером F-Root, мы разработали и поддерживаем программное обеспечение под названием Bv9, которое на протяжении последних трех с половиной десятилетий является одним из основных программных продуктов DNS.

Но многие другие люди им не пользуются. Я видел здесь Андре. Есть создатели других... нет, его здесь нет. Есть производители другого программного обеспечения, которое работает постоянно. Самое замечательное, что, если бы каждый компьютер Dell работал, корневой сервер все равно работал бы, потому что мы все используем разные вещи. Если операционная система рухнула, если завтра умрет Windows, мы будем использовать множество вариантов Unix. Если завтра умрет Bv9, у нас будет множество других приложений. Это потрясающе разнообразная и устойчивая система без единой точки технического отказа.

Кроме того, нет точки институциональной неэффективности, когда вы переживаете: а вдруг у этой компании возникнут проблемы, и она обратится в суд? Что если кто-то подаст на вас в

суд? Что если кто-то скажет, что вы больше не подходите? Что если у вас закончатся деньги? Это не имеет значения. Мы — 12 отдельных организаций. Мы проводим много времени вместе. С некоторыми из этих людей я вижусь чаще, чем с собственными детьми, но мои дети уже взрослые, так что ничего страшного. Мы сотрудничаем, но все мы независимые. Мы — самостоятельные организации, поэтому одно действие, нанесшее вред одной организации, не нанесет вреда всей нашей группе. Нет единой точки институциональной неэффективности.

Кроме того, и это сложновато для новичков в этом деле, но широко распространен слух, что мы, операторы корневых серверов, можем контролировать данные о том, что вы видите. Мы можем контролировать, к кому и куда вы можете попасть. Это очень далеко от истины. Если у вас есть домен, вы можете указать, к чему он подключается, и передать данные своему регистратору, а он передает их группе под названием IANA. IANA помещает их в пакет, и вот этот парень, непосредственно участвующий от организации под названием... он не смотрит. Он работает в организации по обслуживанию корневой зоны. Они упаковывают данные криптографически, так что это абсолютно безопасно. Передают их нам, и мы рассылаем их всем 1758 или сколько их там сейчас.

Корневым серверам по всему миру, и вы все получаете эти данные. Мы их не меняем. Мы к ним не обращаемся. Мы их не корректируем. Мы их не редактируем. Мы берем информацию, которая поступает к нам, и доставляем ее всему миру. Мы делаем это уже 40 лет. В этом

году уже 40 лет как все работает без единого сбоя. За 40 лет система буквально ни разу не выходила из строя. Если вы работали с компьютерами, то понимаете, что это удивительная цифра. И вот еще что интересно, если вы действительно хотите добраться до сути: система адресации, которую мы используем, называется Anycast, и она как бы предотвращает DDoS-атаки. Просто не получится запустить DDoS в зеркале Anycast, чтобы это сломало нормальную работу. Мы никого не просим это делать, но многие пытались, и система не падала.

Итак, система корневых серверов — это действительно важная, пусть и редкая, часть процесса разрешения адресов, которая сегодня используется великое множество раз практически всеми интернет-пользователями на Земле. Большая часть запросов выходит из памяти, а большинство остальных никогда не попадают на корневой сервер. Операторы корневого сервера не контролируют содержимое. Система удивительно прочна, устойчива, разнообразна, она просто работает. Именно так работает система корневых серверов. Большое спасибо.

СИРАНУШ ВАРДАНЯН: Это очень впечатляет, Джефф, очень. Теперь рядом с вами сидит еще один эксперт по DNS. Большое спасибо.

ДЖЕФФ ОСБОРН: Запишите это в свое резюме и попросите прибавки.

СИРАНУШ ВАРДАНЯН: Большое спасибо. Это действительно очень интересно. Есть вопросы? Да, пожалуйста. Филомено, воспользуйтесь тем микрофоном. У нас около семи минут на вопросы к Джеффу, а затем перейдем к SSAC.

ЗОИ ФИЛОМЕНО (ZOE FILOMENO): Здравствуйте, меня зовут Зои Филомено, я участник программы Fellowship ICANN79. Я представляю междисциплинарную область узких технологий — интерфейсы мозг-компьютер для пациентов с дегенеративными заболеваниями.

ДЖЕФФ ОСБОРН: Не могли бы вы ближе подойти к микрофону?

ЗОИ ФИЛОМЕНО: Да. Отлично.

ДЖЕФФ ОСБОРН: Так намного лучше. Прошу прощения.

ЗОИ ФИЛОМЕНО: Итак, пересечение узких технологий, интерфейсов мозг-компьютер и новых технологий. Мой вопрос касается новых

технологий и того, как многие системы повторяют человеческие связи в системе, созданной нами самими. То есть, по сути, я хочу сказать, что вся эта система — это наша собственная нервная система. Дайте мне секундочку. Нервная система, память, то, как мы получаем доступ, — это то, как получают доступ корневые серверы. Поэтому в будущем меня беспокоят пациенты с интерфейсами мозг-компьютер, подключаемыми к интернету. Наступит ли будущее, в котором вы, Джефф, или еще кто-то, сформируете политику в отношении того, как все это работает? Надеюсь, это понятно. Прошу прощения.

ДЖЕФФ ОСБОРН: Это лучший вопрос, который я когда-либо получал в ICANN. Возможно, я недостаточно умен, чтобы ответить на него соответствующим образом. Ну и ну.

ЗОИ ФИЛОМЕНО: Да. Если что, в IANA мне уже сказали, что не собираются заниматься этим вопросом, пока он не станет проблемой дня сегодняшнего.

ДЖЕФФ ОСБОРН: К сожалению, это почти то же самое, что вынужден сказать и я. Это очень интересно — заглянуть в будущее и посмотреть, что произойдет. И я связан с интернетом дольше, чем мне хотелось бы признать. И много раз ошибался, угадывая, что будет дальше.

Никогда не ожидал, что появятся социальные медиа. Это был полный шок. Так что, скорее всего, я ошибусь и в этом случае. Наша работа доставляет огромное удовольствие, потому что мы, большинство людей, с которыми я работаю, поддерживаем работу интернета.

И мы просто в восторге от того, что люди с ним делают. Мы стараемся, чтобы он был надежным. Мы стараемся, чтобы он был быстрым. Мы стараемся, чтобы он был доступен как можно большему числу людей на Земле и работал как можно лучше. А потом мы сидим и смотрим, как люди вроде вас делают с ним невероятные вещи, и говорим: о боже, и мы к этому причастны. Так что я буду наблюдать за тем, что вы делаете, но не знаю, что я смогу сделать, кроме как прикладывать все усилия к тому, чтобы он всегда был рядом, доступен и быстр.

ЗОИ ФИЛОМЕНО: Да. И если позволите, я добавлю к тому, что вы говорили о DDS-атаках. Я специализируюсь на том, как математические алгоритмы в музыке влияют на нейрохимические вещества. Так что это можно использовать для проникновения в человека или его биохакинга, чтобы создавать определенные ситуации. Если это верно в отношении того, как вы действуете, то это может означать, что, если у вас нет проблем с DDS-атаками, это может быть верно и для пациентов с имплантатами. Так что я вроде...

ДЖЕФФ ОСБОРН: Интересные параллели. Мой сын пытается поступить в медицинский вуз. У меня есть соображения по этому поводу, и их действительно трудно высказать перед сотней людей, но вопрос очень интересный. Если вы найдете меня в коридоре, я угощу вас кофе, и мы поговорим об этом. Это очень интересно.

ЗОИ ФИЛОМЕНО: Спасибо.

ДЖЕФФ ОСБОРН: Конечно. Спасибо.

СИРАНУШ ВАРДАНЯН: Шанель, прошу вас.

ШАНЕЛЬ МАКФЕРСОН (SHANELLE MCPHERSON): Да. Добрый день! Всех приветствую! Меня зовут Шанель Макферсон, я участник программы Fellowship ICANN79 и выступаю от своего имени. Прежде всего, мы все только что с отличием завершили обучение. Благодарю вас. Это первое. Мой вопрос, и мне просто любопытно. Я хотела бы знать, если речь идет о новых gTLD, которые скоро появятся, они уже встроены в сервер или они создаются из корня. Если появляется новый gTLD, как сервер узнает, что он уже есть? Создается ли он в корне? Это мой вопрос.

ДЖЕФФ ОСБОРН: Замечательный вопрос.

ШАНЕЛЬ МАКФЕРСОН: Да. Спасибо.

ДЖЕФФ ОСБОРН: Корневая зона — это, по сути, список всех TLD, а адрес для них фактически один в IPv4 — это версия адресации, которую я использовал здесь, а также IPv6 — более длинный, новый способ адресации. Как правило, примерно два раза в день создается новый файл корневой зоны. Поэтому, когда появляются новые TLD, они просто добавляются в список, и все. Как только он генерируется, дважды в день, он отправляется. Они могут прислать им еще. На днях кто-то рассказывал мне, что это произошло пять раз, а не два. Это очень быстро, и все это становится частью корневой зоны. Хороший вопрос.

НЕИЗВЕСТНЫЙ ОРАТОР: [неразборчиво — 0:28:22], участник программы Fellowship ICANN. Мой вопрос заключается в том, какие методы и системы в системе корневого сервера с точки зрения защиты и мониторинга, используются для проверки работоспособности и производительности всех систем корневого сервера... знаю, что есть защита на случай сбоя, но какие системы используются с точки зрения производительности?

ДЖЕФФ ОСБОРН: В связи с корневым сервером, вот что любопытно и почему мы пытаемся напомнить людям о том, как редко он используется: он не влияет на задержку сигнала, которую бы заметили люди в течение своего обычного дня. Вспомните, когда вы в последний раз искали что-то и вводили URL. Представьте, сколько времени у вас уйдет на то, чтобы сделать это в 5000-й раз. Предположим, что ближайший к вам корневой сервер вышел из строя. Следующий, вероятно, находится на расстоянии нескольких миллисекунд. Когда вы 5000-й раз ищете что-то, время поиска увеличится еще на 5 миллисекунд. Какова вероятность того, что вы это заметите? Это буквально настолько редко используемая функция, которая после того, как вы один раз ее использовали, просто попадает в кэш, и очень трудно понять, как конечный пользователь может заметить не то что медленный корневой сервер, а даже неработающий.

Потому что их очень много. Когда я сказал, что DDoS-атаки не работают, мы используем очень интересную штуку под названием Anycast. Представьте, что у вас есть ресторан с тысячей официантов по имени Хосе. Если вы поднимете голову и скажете: «Эй, Хосе!», официант всегда найдется. Если он уйдет на кухню, то неважно, позовете ли вы Хосе, потому что есть еще. Поскольку все реплики сервера F-Root по всему миру, а их в моей компании почти 300, имеют один и тот же адрес, то, когда вы говорите: «Эй, сервер F-Root», неважно, что один из них мертв. Есть еще один через 50 миль от него, и еще через 50 миль, и еще.

Интернет будет продолжать работать, пока не найдется тот, который работает. Уйдут буквально миллисекунды дополнительного времени. Мы очень много чего делаем независимо друг от друга, и у каждой организации есть свои способы обеспечить непрерывную работу. Мы очень гордимся тем, как мы работаем, но мы все действуем по-разному, потому что нам не нужна монокультура, в которой один недостаток, одна ошибка или одна проблема уничтожает больше, чем одну вещь. Понимаете?

НЕИЗВЕСТНЫЙ ОРАТОР: Конечно. Спасибо.

ДЖЕФФ ОСБОРН: Хорошо. Спасибо за помощь.

СИРАНУШ ВАРДАНЯН: Ребята, сейчас у нас нет времени на вопросы, потому что пора переходить к презентации SSAC. Не хотите подождать до конца сессии, тогда у нас будет время для вопросов и Джефф останется здесь?

ОЛОРУНДАРЕ ДЖЕЙМС КУНЛЕ (OLORUNDARE JAMES KUNLE): Так после меня или?..

СИРАНУШ ВАРДАНЯН: Нет, включая вас, но если уложитесь в 30 секунд, то пожалуйста.

ОЛОРУНДАРЕ ДЖЕЙМС КУНЛЕ: О, абсолютно. Хорошо. Меня зовут Кунле.

СИРАНУШ ВАРДАНЯН: Я позабочусь о том, чтобы наш участник программы NextGen первым задал вопрос.

ОЛОРУНДАРЕ ДЖЕЙМС КУНЛЕ: Вопрос следующий. Простите, возможно, я пропустил, когда выходил в Истман. Речь о том, кто может вступить в RSSAC, а кто нет, и каковы условия вступления? Спасибо.

ДЖЕФФ ОСБОРН: В состав RSSAC входят по два представителя от каждой из 12 организаций, которые его обслуживают, а также есть группа подготовки RSSAC, в которую входят эксперты DNS со всего мира. Чтобы стать членом RSSAC, вам необходимо управлять одним из корневых серверов. Чтобы стать членом группы подготовки RSSAC, я фактически являюсь председателем комитета по членству в группе подготовки RSSAC. Вы должны

продемонстрировать, что обладаете практическими знаниями DNS, потому что мы не проводим обучение. Мы собираем группу экспертов, которые выполняют большую часть работы. Большую часть работы RSSAC выполняет группа подготовки, а это разнообразная группа людей со всего мира. Их много среди присутствующих. Я бы поискал, но мне мешает свет. Все, что вам нужно, — это иметь хорошие практические знания DNS и подать заявку.

Она попадет прямо ко мне и еще шести ребятам, которые ее посмотрят и решат. Если у вас недостаточно опыта, мы посоветуем показать нам, в чем, по вашему мнению, у вас хороший опыт. Если это не сработает, мы можем сделать вас участником только листа рассылки, и вы сможете работать до тех пор, пока не почувствуете, что достаточно научились и теперь знаете, как и что делать. Это очень инклюзивная группа. Нам действительно нужна помощь, но это не обучающая организация. Нам нужны готовые эксперты, потому что именно так выполняется большая часть работы. Мое пояснение помогло?

СИРАНУШ ВАРДАНЯН: Спасибо. Джефф Осборн, председатель RSSAC. Большое спасибо. Ваши аплодисменты адресованы Джеффу, но Джефф, прошу вас остаться. А сейчас я с большим удовольствием представляю вам председателя и заместителя председателя SSAC, Рама Мохана (Ram Mohan) и Тару Уэйлен (Tara Whalen). Рам, я так рада видеть вас на программе Fellowship. Когда я была участником программы,

именно вы проводили презентацию для сообщества, и мне очень понравилось, так что спасибо, что пришли. Вам слово.

РАМ МОХАН: Большое спасибо. И доброго вечера всем собравшимся. Мне очень приятно находиться здесь. Спасибо, что пригласили нас с Тарой. Прежде чем приступить к презентации, я хочу рассказать вам одну историю. Это история SSAC. С 1990-х годов, еще до того, как многие из вас родились, присутствовала обеспокоенность по поводу атак на критическую инфраструктуру интернета, террористических атак на критическую инфраструктуру интернета. Это было проблемой довольно долгое время. Люди собирались и говорили об этом, а потом расходились. Они говорили: это важно. Может быть, нам стоит следить за этим, стоит продолжать.

А потом в 2001 году случилось 11 сентября. Это была целенаправленная атака, но не на инфраструктуру интернета, а на другие виды инфраструктуры, произошли другие вещи. И это действительно повысило глобальную осведомленность о том, что, если бы террористы, помимо всех остальных своих деяний, атаковали бы критическую инфраструктуру интернета, это принесло бы еще больше разрушений и проблем. После событий сентября 2001 года, в ноябре 2001 года ICANN провела встречу в Марина-дель-Рей, в Калифорнии, где некоторые из тех, кто работал в ICANN, и тех, кто также помогал координировать общие правительственные меры реагирования на террористические атаки, собрались вместе и привлекли к участию нескольких из нас,

которые занимались непосредственным управлением критической инфраструктурой.

В то время моя компания, а я был техническим директором этой компании, управляла доменом верхнего уровня .info, который был новым доменом, но все же значительной его частью. В компании VeriSign были люди, которые управляли не только корневыми серверами, но и доменами .com, .net и .org. Другие люди, которые управляли национальными доменами, собрали нас вместе и сказали: только представьте, что будет, если произойдет атака и ваши домены захватят или уничтожат. Потому что до этого момента, хотя и присутствовала некоторая обеспокоенность, все же казалось, что все должно быть хорошо. Все мы хорошие люди, работаем из лучших побуждений, и все должно быть хорошо. Построим достойную защиту, создадим достойные системы, а о многом другом беспокоиться не обязательно.

В 2001 году мы в ICANN организовали новую группу. Вначале нас было всего шестеро, но мы назвали себя Консультативным комитетом по безопасности и стабильности. В 2002 году он фактически приобрел официальный статус. Правление ICANN собралось и сказало: мы считаем, что важно иметь группу, состоящую из экспертов, которые понимают основы технологии DNS, понимают основы работы DNS, собираются вместе, и поставить перед ними четкую цель. Именно это и привело к созданию SSAC. У ICANN есть своя миссия, и эта миссия гласит, что она создана для обеспечения стабильной и безопасной работы

систем уникальных идентификаторов в интернете. Стабильность и безопасность — вот что лежит в основе миссии SSAC.

В чем же заключается наша роль? Мы рассматриваем вопросы, которые касаются безопасности и целостности всей системы распределения имен и адресов Интернета, и мы собрали группу экспертов, которые разбираются в этих вопросах. Мы собираемся вместе, работаем вместе, а затем выдаем рекомендации. Номинально эти рекомендации адресованы Правлению, но на самом деле они адресованы Правлению и сообществу. Вот что действительно интересно в том, что мы делаем. Мы — консультативный комитет. Мы только даем рекомендации. Правление ICANN должно прислушаться к нашим рекомендациям. Они могут их просто проигнорировать. Они могут не воспользоваться ими, если захотят. Ни в уставе, нигде нет требований к Правлению ICANN действовать в соответствии с нашими рекомендациями.

Это действительно замечательная особенность, потому что, скажу я вам, это означает, что мы, SSAC, несем огромную ответственность за то, что любая наша рекомендация подкреплена данными. Она подкреплена реальными фактами, которые мы наблюдали в реальном мире. Это не просто кучка людей, которые хотят собраться вместе и сказать, что небо падает. Наш авторитет основан на моделировании на основе данных, анализе на основе данных, а в некоторых случаях и на анализе на основе накопленного опыта. Это означает, что мы также не

связываем ICANN и правление своими советами и рекомендациями, потому что в некоторых случаях наши советы могут быть слишком жесткими и их невозможно реализовать в системе ICANN.

В других случаях наши советы могут оказаться недостаточными. Это дает некоторую свободу действий, но самое главное для нас, членов SSAC, заключается в том, что, поскольку мы являемся консультативным комитетом, не имеющим полномочий по принудительной реализации чего бы то ни было внутри этого сообщества, это поднимает планку для нас: мы должны выдавать рекомендации, которые действительно являются достойными, выполнимыми, основанными на данных и фактах. На этом слайде довольно много написано, но я остановлюсь лишь на некоторых моментах. Что мы делаем? Мы взаимодействуем с техническим сообществом, с тем, которое занимается инфраструктурой DNS, с тем, которое занимается требованиями безопасности. Но когда я говорю «техническое сообщество», я также имею в виду людей, занимающихся политикой. Я также имею в виду людей, которые занимаются законодательством.

Таким образом, мы взаимодействуем с массой людей, у которых есть большой интерес к DNS и безопасности DNS. После общения с ними мы анализируем риски и угрозы для систем распределения имен и адресов в Интернете. Мы формируем группы внутри SSAC, и часто у нас нет всех необходимых знаний и опыта, поэтому мы обращаемся к экспертам и приглашаем их работать с нами. Это

означает, что те, кто входит в SSAC, кто работает с SSAC, часто общаются, ведут серьезные разговоры с людьми, которые создают технологии, протоколы, системы, обеспечивающие работу интернета, DNS в том виде, в каком они представлены сегодня.

После этого мы координируем свои действия с различными техническими и другими организациями и приходим к заключению по любой рассматриваемой теме. Приведу пример. Недавно мы рассматривали вопрос о том, что происходит с блокчейн-именами, которые находятся в блокчейне. Что происходит с другими видами имен, которые развиваются в общей экосистеме? Какое влияние это оказывает на DNS. Мы собрали группу людей, у которых есть к этому интерес и опыт. Мы работали над этим около года и опубликовали отчет. Этот отчет находится в открытом доступе, в нем содержатся замечания, рекомендации, с которыми может ознакомиться сообщество, а также он предназначен для Правления. И это те вещи, которые мы делаем на регулярной основе. Это то, чем занимается SSAC, и если вы посмотрите на членов SSAC, то это действительно руководство SSAC.

В руководство SSAC избраны несколько человек. Я — председатель. Тара, сидящая справа от меня, — заместитель председателя. Джим Галвин (Jim Galvin) — наш представитель в правлении ICANN, и Джефф Бедсер (Jeff Bedser) и Барри Либа (Barry Lieba) — два уважаемых коллеги, которые также входят в команду руководителей. Но мы смотрим на это так: SSAC и работа, которую

мы выполняем, невозможны без людей по ту сторону экрана, замечательного вспомогательного персонала, который у нас есть. Вот Стив, вот Даниэль, Кэти и Моузес, и между нами, в нижней части экрана вы видите наши наборы навыков и опыта. В SSAC есть еще примерно 30 человек, которые обладают другими навыками, другими знаниями и опытом.

Вкратце, не буду вдаваться в подробности. Эти слайды будут доступны вам, но на данном слайде показана как широта, так и глубина вопросов, которые мы рассматриваем. Как видите, безопасность DNS — предмет нашего особого внимания. Мы много чего сделали в плане безопасности DNS, но мы также писали о глобальном пространстве имен, доменах без точки, доменных коллизиях, совместном использовании доменных имен и других вещах. Мы только что опубликовали отчет о том, что имя нельзя передавать в общественное пользование, потому что оно должно использоваться сетями для внутренних целей.

Мы только что опубликовали отчет об этом. Наши усилия были сосредоточены на регистрационных данных, интернационализированных доменных именах, проблемах универсального принятия, вариантах и защите маршрутизации. Это широкий диапазон интересов, но если посмотреть на них, то в центре внимания в основном имена и адреса. Мы не комментируем, хорош или плох спам. Мы не комментируем социальные сети, вещи на уровне приложений. Основное

внимание мы уделяем тому, что находится на уровне DNS в интернете.

Так что это и есть SSAC. Для некоторых энтузиастов это очень увлекательно. А для многих других получателей наших консультаций мы очень стараемся сделать их удобоваримыми, доступными и понятными, и при этом говорить с людьми не свысока. То, что вы эксперт, не означает, что вы должны кичиться своими знаниями. На самом деле, лучший способ стать экспертом — это сделать этот опыт доступным и понятным как можно большему количеству людей. Вот кто работает в SSAC. Теперь я передам слово Таре, которая расскажет о том, что такое SSAC и чем мы занимаемся. Тара здесь, чтобы рассказать о SSAC.

ТАРА УЭЙЛЕН: Здравствуйте! Как заместитель председателя, я также являюсь председателем комиссии по приему в члены, поэтому я очень рада выступить перед потенциальным пулом кандидатов, которые могут стать членами в будущем. Одной из наших целей является диверсификация членства, и мы, конечно, смотрим в будущее, потому что нам нужно поддерживать наше членство в течение долгого времени. Поэтому я также рада возможности поговорить с людьми, которые находятся в самом начале своего пути в ICANN. В зависимости от того, чего вы достигли в своей профессиональной деятельности, возможно, у вас уже есть некий опыт. Возможно, в ближайшем будущем у вас появится такая возможность, а может быть, вы заглядываете немного дальше и

считаете, что SSAC и тип работы, которую они выполняют, могут быть вам интересны.

Поэтому мы хотим наладить с вами контакт, чтобы эти возможности воплотились в жизнь. Сегодня я хочу немного рассказать о наших конкретных целях по обеспечению разнообразия, которые мы поставили перед собой, о том, специалистов с какими навыками и опытом мы ищем, а также о том, почему вам может быть интересно присоединиться к нам и что это вам даст, и, конечно же, о том, как вы можете связаться с нами и найти способ вступить в наши ряды.

СИРАНУШ ВАРДАНЯН: Тара, просто напомню, что осталось 10 минут.

ТАРА УЭЙЛЕН: Десять. Большое спасибо.

СИРАНУШ ВАРДАНЯН: У нас 10 минут.

ТАРА УЭЙЛЕН: Конечно. Итак, это наши цели в области обеспечения разнообразия. Нам очень нужны разные точки зрения и уникальные взгляды. Как отметил Рам, у нас довольно широкий спектр тем, которые мы рассматриваем в рамках огромной сферы

безопасности и стабильности. Мы сталкиваемся с проблемами по всему глобальному интернету, но помните, что мы говорим о глобальном, и у нас есть области географического разнообразия, в которых мы чувствуем себя слабыми. Мы в значительной степени ориентированы на Северную Америку и Европу, поэтому нам бы очень хотелось распространить охват и на другие регионы мира, Африку, Латинскую Америку и Азиатско-Тихоокеанский регион.

Возможно, у нас здесь есть люди из научных или исследовательских кругов, студенты, которые привыкли анализировать данные, проводить различные виды измерений интернета. У вас есть знания, которые могут оказаться очень полезными для работы SSAC. Мы также следим за гендерным балансом, поэтому я буду очень рада, если к SSAC присоединятся другие женщины. Конечно, мы снова движемся в будущее, поскольку время идет вперед. Нам нравятся люди, которые, возможно, находятся на более раннем этапе своей карьеры, которые готовы и хотят присоединиться к нам.

Это облако слов дает представление о том, чего мы ожидаем от новичков. Здесь много тем, очень технических тем, взятых из нашего опроса о навыках. Вы можете видеть, что здесь явно присутствуют аспекты безопасности и нетворкинга. Возможно, вы работали в определенной области нетворкинга, в определенной форме операций. Возможно, у вас есть опыт работы с аспектами безопасности, связанными с киберпреступностью, или в области управления рисками. Многие аспекты вопросов стабильности и

безопасности имеют отношение к нам и нашей работе. Вы можете увидеть себя в некоторых из этих областей знаний. Оглянитесь вокруг, в частности, изучите документы и то, чем мы занимаемся, и подумайте, может быть, вы сможете внести свой вклад.

Опять же, почему вы хотите присоединиться к нам? Думаю, Рам также отметил некоторые из интересных моментов и то, чем вы могли бы заняться. Мы работаем над очень важными вопросами безопасности. Если вы любите погружаться в работу и заниматься сложными вопросами, у нас в SSAC нет недостатка в такой работе. Вы сможете расширить свои знания в других областях, связанных с интернетом в целом, глобальными проблемами интернета, крупномасштабными вопросами, работая над этими проблемами с различными специалистами в области безопасности. Вы наверняка сочтете это полезным для карьерного роста и углубления собственных знаний. Многие формы обеспечения безопасности понятны, потому что эта работа имеет такое влияние в мировом масштабе.

И, конечно же, экспертиза позволяет улучшить работу интернет-систем. Таким образом, вы консультируете правление и сообщество DNS во всем мире, чтобы сделать работу более безопасной и стабильной и внести вклад в выполнение миссии. Так что, если вы чувствуете, что хотите заниматься именно этим, мы настоятельно рекомендуем вам подать заявку на вступление. У нас есть материалы на сайте и онлайн-заявка, в которой изложен весь этот материал. Но я также хочу отметить, что в этом году мы

пробуем кое-что новое и проводим открытый форум. У нас будет заседание в четверг, блок 1.

И это возможность для вас пообщаться с нами напрямую, дать нам немного больше времени, чтобы вы могли поговорить с нами с глазу на глаз, задать больше вопросов, узнать подробнее о проектах, над которыми мы работаем, и о работе, которую мы планируем, и просто в целом познакомиться с нами и узнать, что мы из себя представляем, потому что мы понимаем, что это тоже очень важно. Поэтому рекомендуем вам посетить это заседание, но мы также готовы поговорить с вами в любое время. Поэтому, пожалуйста, связывайтесь с нами, мы будем рады пообщаться. Спасибо.

СИРАНУШ ВАРДАНЯН: Спасибо. Я с нетерпением жду этого заседания, на которое придут обе группы. Потому что мы, участники программ Fellowship и NextGen, всегда очень интересуемся аспектами безопасности, и нам всегда кажется, что мы стоим перед закрытыми дверями. Но сейчас я счастлива, что ваши двери открыты для нас. У нас здесь есть настоящие таланты. И я уверена, что после 15 лет действия программы Fellowship у нас в SSAC наконец-то есть один член, который пришел из программы Fellowship, и мы гордимся этим. Но у нас в этой группе есть множество людей одаренных и способных, которые заинтересованы в том, чтобы присоединиться. Так что спасибо вам за презентации.

Я также хотела бы поблагодарить Джеффа за то, что он назначил члена отборочной комиссии и ментора для программы Fellowship. Не могу объяснить, насколько важны ваши знания и опыт в отборе и наставничестве. Я призываю SSAC также следовать этим шагам. Я обещала, что право задать первый вопрос участникам программы NextGen, а последний — вам, но я хотела бы сдержать обещание. Так что вопрос от вас. Говорите. Вам слово.

РАШИД ХАССАН (RASHID HASSAN): Спасибо за эту возможность. Я Рашид Хассан. Я участник программы NextGen. У меня вопрос к Джеффу. У меня два вопроса. Итак, первый вопрос — технический. В системе DNS есть запись под названием CNAME, и у многих компаний есть запись CNAME, и они просто хранят ее в целях ведения учета и для некоторых других операций. Однако по окончании операции забывают удалить ресурс, но запись DNS остается. Из-за этого возникает атака под названием захват через CNAME или захват домена. Это делают хакеры и говорят: я взломал Google. Вы не взломали Google. Вы просто использовали CNAME.

Так что на уровне политики, к примеру, рекомендуете ли вы компаниям или ICANN на случай, если я не использую запись CNAME, сколько времени я должен ее хранить, что я должен с ней делать и как быстро я должен ее уничтожить? Потому что это просто технический вопрос. И второе, допустим я хочу присоединиться к RSSAC, я уверен, что там есть много документов White Paper, ресурсов и много чего еще. Есть ли у вас что-нибудь в

инфографическом варианте или в кратком изложении, чтобы я, ознакомившись, мог легко понять работу? Вот. Спасибо.

ДЖЕФФ ОСБОРН: Спасибо за вопрос. Позвольте мне сначала ответить на второй вопрос. Если вы буквально наберете в Google «присоединиться к группе подготовки RSSAC», думаю, вы прямо там и окажетесь. Это на сайте ICANN, и это действительно отличный процесс. Там легко заполнить заявку. Там описаны наши требования, в чем заключается работа. Как я уже сказал, это хороший процесс, в котором, если у вас пока нет того опыта, который, по нашему мнению, важен для того, чтобы вы могли стать ценным рабочим членом, вам предлагают место наблюдателя или участие в листе рассылки, и в какой-то момент, возможно, вы почувствуете, что достаточно в этом разобрались. Возвращайтесь и спрашивайте. Но это не столько функция обучения, фактическое членство — это группа, которая выполняет реальную работу. Мы делаем реальные вещи. И поэтому наблюдать за ней интересно.

Так что я бы буквально сказал, что через Google вы моментально там окажетесь. Я старался, чтобы люди могли легко это найти. Google работает. Что касается того, как долго хранить CNAME, то это выходит за рамки того, что делает система корневого сервера. И замечу, что вы можете попробовать найти лучшего эксперта, чем я. Уэс, например, здесь, или Питер. Хотите подойти к микрофону и ответить? Питер — член группы подготовки RSSAC, а также SSAC, я думаю.

ПИТЕР ТОМАССЕН (PETER THOMASSEN): Очень кратко. Я один из молодых членов SSAC. Что касается записи CNAME, когда вы больше ее не используете, она по-прежнему указывает на цель, потому что CNAME — это, по сути, запись псевдонима. Так что проблема возникает только в том случае, если незаметно для вас целевое имя хоста переходит под контроль кого-то другого. Обычно это происходит не за день, но если вы забудете проверить, то проблема может возникнуть позже. Поэтому рекомендация такова: не храните ненужные вещи. Не ставьте в доме ненужные двери. И просто удалите псевдоним, если он вам больше не нужен. Но это не значит, что если вы оставите его, то он сразу же станет проблемой. Он становится проблемой только тогда, когда цель меняет контроль.

СИРАНУШ ВАРДАНЯН: Большое спасибо. И последний вопрос будет от вас, Эсау, и мы подведем итоги.

ЭСАУ ТУПОУ (ESAU TUPOU): Спасибо. Я участник программы Fellowship ICANN и выступаю от своего имени. Насколько я понимаю, интернет начинался как оборонный проект. Могу ошибаться, но вроде как оборонный проект. И по проекту в нем не было концепции безопасности. А потом у него появилась функция обмена информацией, а также связи. Но теперь все меняется, в том числе и обычная

преступность. Теперь у нас есть киберпреступность и все остальное. Поэтому мой вопрос к SSAC: работаете ли вы с другими сторонами над регулированием, а также над правами человека и прочим, чтобы обеспечить безопасность? Спасибо.

РАМ МОХАН: Большое спасибо. Это отличный вопрос. Мы поддерживаем связь с правительствами, с людьми из правительств. Некоторые из наших членов работают в государственных структурах. Но мы также напрямую работаем внутри ICANN. Например, мы напрямую работаем с людьми из Правительственного консультативного комитета. А внутри Правительственного консультативного комитета есть подгруппа под названием Рабочая группа по обеспечению общественной безопасности. В нее обычно входят люди, которые являются не только управленцами, но и иногда полицейскими или прочими подобными людьми, цель которых — обеспечивать стабильность и правопорядок также и в интернете.

Поэтому мы довольно регулярно и активно взаимодействуем с ними. Многие наши члены также принимают участие. Во всем мире существуют группы реагирования на инциденты информационной безопасности, группы CERT. И у нас есть члены, которые участвуют в их работе. Также есть вышестоящая организация FIRST, с которой мы тоже сотрудничаем.

СИРАНУШ ВАРДАНЯН: Большое спасибо. Давайте поаплодируем нашим докладчикам. Большое спасибо, что пришли к нам сегодня. Это отличное завершение второго дня в ICANN. Большое спасибо. На этом объявляю наше заседание закрытым. Увидимся завтра на приветственной церемонии. Спасибо. Спасибо, это было здорово.

[КОНЕЦ СТЕНОГРАММЫ]