САН-ХУАН — совместное заседание: Правление ICANN и RSSAC
Четверг, 15 марта 2018 года, 10:30 – 11:30 по AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

КАВЕ РАНДЖБАР (KAVEH RANJBAR): Мы начнем через две минуты.

Давид, пожалуйста, сядьте за стол. Большое спасибо.

Хорошо. Давайте начнем заседание. Йонне, пожалуйста, присаживайтесь к главному столу.

Итак, начнем заседание.

Кого-то из присутствующих членов RSSAC или Правления еще нет за главным столом? У нас остались свободные места. Присоединяйтесь к сидящим за главным столом, если еще не сделали этого.

Всем доброе утро.

Добро пожаловать на открытое совместное заседание Правления ICANN и RSSAC. Позвольте начать с быстрой переклички, а затем мы рассмотрим вопросы, включенные в повестку дня.

Начну с Джорджа, если не возражаете? Джордж, представьтесь, пожалуйста.

ДЖОРДЖ САДОВСКИ (GEORGE SADOWSKY): Джордж Садовски.

ДАВИД КОНРАД (DAVID CONRAD): Давид Конрад, технический директор ICANN.

АВРИ ДОРИА (AVRI DORIA): Аври Дориа, Правление ICANN.

РАЙАН СТЕФЕНСОН (RYAN STEPHENSON): Райан Стефенсон, RSSAC, DOD.

ЙОННЕ СОЙНИНЕН (JONNE SOININEN): Йонне Сойнинен, представитель IETF в Правлении ICANN.

ЛИТО ИБАРРА (LITO IBARRA): Лито Ибарра, Правление ICANN.

КАВЕ РАНДЖБАР: Каве Ранджбар, представитель RSSAC в Правлении ICANN.

БРЭД ВЕРД (BRAD VERD): Брэд Верд, сопредседатель RSSAC.

ТРИПТИ СИНХА (TRIPTI SINHA): Трипти Синха, сопредседатель RSSAC.

ШЕРИН ШАЛАБИ (CHERINE CHALABY): Шерин Шалаби, Правление ICANN.

КРИС ДИССПЕЙН (CHRIS DISSPAIN): Крис Дисспейн, Правление ICANN.

БЕККИ БЕРР (BECKY BURR): Бекки Берр, Правление ICANN.

РАМ МОХАН (RAM MOHAN): Рам Мохан, представитель SSAC в Правлении ICANN.

ДЖЕФФ ОСБОРН (JEFF OSBORN): Джефф Осборн, член RSSAC.

ДАНИЭЛЬ МИГО (DANIEL MIGAULT): Даниэль Миго, представитель IETF в RSSAC.

ЙОРАН МАРБИ (GORAN MARBY): Йоран Марби, корпорация ICANN.

КАВЕ РАНДЖБАР: Большое спасибо.

РАСС МАНДИ (RUSS MUNDY): И Расс Манди, представитель SSAC в RSSAC. Извините, я запыхался.

КАВЕ РАНДЖБАР: Добро пожаловать, Расс.

БРЭД ВЕРД: И некоторые из отсутствующих членов RSSAC прислали извинения. Многие из них уже в самолете и торопятся в Лондон на мероприятие IETF. Хочу извиниться от их имени.

КАВЕ РАНДЖБАР: Спасибо, Брэд.

Прежде чем мы приступим к рассмотрению вопросов, хочу задать тон этому совещанию. Оно носит неофициальный характер — это встреча членов Правления с RSSAC. Но мы предпочитаем сохранять неофициальный тон во время диалога между членами Правления и членами RSSAC. У нас уже есть ряд вопросов. Мы их рассмотрим. Хочу подчеркнуть, что они по нашему замыслу должны определить характер и

структуру обсуждения. Но мы действительно хотим вести диалог. Мнения, которые прозвучат здесь, могут быть мнениями частных лиц, отдельных членов RSSAC. Это следует отметить. То же самое относится и к Правлению. Мы не собираемся принимать какие-либо решения. Как обычно, решения будут приняты на основании официальных рекомендаций, которые RSSAC даст Правлению. По-моему, этот час дает прекрасную возможность для получения разъяснений. Если у членов Правления имеются вопросы или комментарии, сейчас подходящее время для того, чтобы внести ясность.

А теперь давайте перейдем к следующему слайду.

Это вопросы Правления ICANN, адресованные RSSAC. По существу, было два вопроса. Мы начнем с первого.

Каковы основные цели RSSAC на 2018 год? Об этом я попрошу рассказать председателей.

ТРИПТИ СИНХА: Спасибо, Каве. И спасибо за эти вопросы.

Что касается наших основных целей на 2018 год, то их три. И я начну с первой.

Как известно некоторым из вас, уже почти три года мы работаем над ключевыми рекомендациями Правлению относительно следующего этапа развития системы корневых серверов. Она была введена в действие много

десятилетий назад. И все это время ее модель практически не менялась и не развивалась.

Поэтому мы потратили приличное количество времени на углубленное изучение этой модели, стремясь найти ответы на ряд вопросов, которые уже много лет остаются открытыми, таких как встроенные в систему меры по обеспечению подотчетности. Кому мы подотчетны? Кто заинтересованные стороны? Как система финансируется? Как поддерживается? Как она будет продолжать расти и наращивать свой масштаб в соответствии с темпами постоянного роста интернета?

И мы очень близки к завершению подготовки своих рекомендаций. В соответствии с нашим графиком работы уже есть предварительная версия. Мы намерены подготовить версию, которая будет очень близка к окончательной, в мае на семинаре RSSAC.

Мы собираемся рассказать о той версии Правлению на вашем семинаре, а в июне окончательно доработать ее и вынести на голосование.

Таким образом, в настоящий момент, если не учитывать возможные непредвиденные проблемы и задержки, мы передадим свои рекомендации на конференции ICANN 62. И это наше основное направление работы на данный момент.

Второе направление нашей работы связано с тем, что недавно, как вам известно, началась проверка комитета. И в настоящий момент она еще идет. Скорее всего, она завершится в апреле. После проверки мы получим рекомендации. И будем прорабатывать эти рекомендации с соответствующими комитетами.

Кроме того, у нас есть группа подготовки RSSAC, которая занимается многочисленными и разнообразными техническими вопросами. Таким образом, сейчас у нас, грубо говоря, есть три направления работы.

И работа в этих трех актуальных областях — наша главная цель на 2018 календарный год.

ШЕРИН ШАЛАБИ: У меня вопрос.

ТРИПТИ СИНХА: Разумеется.

ШЕРИН ШАЛАБИ: Извините, Трипти. Рекомендации, сроки, вы собираетесь их дать на ICANN 62. Да? Вы сказали, что хотите заранее в неформальной обстановке рассказать о них Правлению?

ТРИПТИ СИНХА: Да. Мы планируем рассказать вам о них на семинаре в Ванкувере, если удастся включить этот вопрос в повестку дня.

ШЕРИН ШАЛАБИ: Отлично. Ваш вопрос будет в повестке дня. Да, это хорошо.

КАВЕ РАНДЖБАР: Мы уже попросили выделить на это время.

ШЕРИН ШАЛАБИ: Именно так. Я помню. Прошу прощения. Что касается проверки SSAC... извините, проверки RSSAC. На сегодняшний день у вас есть комментарии касательно эффективности этой проверки? Какова ваша реакция?

ТРИПТИ СИНХА: По нашему пониманию, эта проверка была организационной. Предметом проверки должен был являться RSSAC, консультативный комитет, динамика его развития и его долгосрочная задача в экосистеме ICANN.

И мы почувствовали, что цель проверки не была достигнута. Это не было организационной проверкой RSSAC, и возникла некоторая... я сказала бы, что в настоящий момент в сообществе нет единого понимания того, что такое RSSAC и какова его роль, и какие еще

члены сообщества формируют RSSAC, определяют RSSAC. Это RSO — операторы корневых серверов. Но, по нашему мнению, это не было организационной проверкой как таковой.

ШЕРИН ШАЛАБИ: Я задал свой вопрос, потому что мы часто слышим мнения различных представителей сообщества и групп интересов об эффективности проверок. И, кажется, через эти комментарии красной нитью проходит мысль о необходимости в первую очередь оценить количество проверок в конкретном году и постараться разнести их по возможности, чтобы каждая стала эффективнее, а не выполнять параллельно довольно много проверок в течение одного года. Так, например, на следующий год запланировано девять проверок. Правильно?

Готов ли RSSAC поддержать мнение почти всех остальных, кто говорит одно и то же, рассматривая все в целом, знаете ли, спрашивает: хватит ли нам добровольцев, чтобы все сделать? Хватит ли нам ресурсов, чтобы выполнить все эти проверки за один год? И не следует ли выполнить их поэтапно за два или может быть за три года: сделать меньше, но добиться большего успеха?

ТРИПТИ СИНХА: Целиком согласна с вами. Фактически, мы хотели бы внести определенный вклад. И мы действительно полагаем, что нужно рассматривать этот процесс целостно. Учитывать также и эффективность проверок. Какова цель и желательный результат? Думаю, что вы должны установить больше направляющих, которые регламентируют проведение этих проверок. Гарантируют соблюдение установленных рамок, очень строго определяют объем проверок. И тон отчетов... отчеты должны носить информативный и конструктивный характер.

ШЕРИН ШАЛАБИ: Хорошо. Йоран... извините, что касается проверок, вы планируете опубликовать документ для консультаций после... каков ваш план? Как получить дополнительные комментарии?

ЙОРАН МАРБИ: Спасибо, Шерин. Это Йоран.

Здесь следует обсудить в общем-то две разные темы. Одна из них — это обязательные проверки, закрепленные в Уставе. Их периодичность.

Когда их нужно начинать и когда прекращать. Это своего рода отдельная тема для обсуждения.

И я намерен... при поддержке со стороны сообщества, распространить определенную информацию. Поскольку это... если мы собираемся что-то сделать, то это будет прямым изменением Устава.

И другая тема, которую вы поднимаете... по-моему, это тоже очень важный вопрос, который понимался не только вами: каковы цели этих проверок?

Для чего они нужны? Насколько эффективны?

И я знаю, что в OEC обсуждение этого тоже началось.

У меня пока нет плана относительно этой части. И не должно быть, потому что этим занимается OEC в Правлении. И будет организован диалогом с сообществом. Но на этой неделе такой вопрос мне неоднократно задавали. Поскольку мы тратим много... извините. Мы тратим много денег и времени непосредственно на проверки. И некоторые проверки продолжаются в организационном отношении... некоторые проверки продолжаются уже очень долго. По-моему, проверка At-Large длится уже четыре года. И это другая тема для обсуждения.

И что касается этого конкретного вопроса, Шерин, я должен сформулировать его и обратиться к OEC, провести переговоры с Правлением. И, как ни удивительно, есть председатель. Он может продолжить. Спасибо.

КАВЕ РАНДЖБАР: Выступит Брэд, затем Халед.

БРЭД ВЕРД: Я хотел сказать, что RSSAC готовит два ответа. Один предназначен для независимой аудиторской компании в надежде... это наш отзыв о выполненной оценке в надежде на то, что пока еще не полученные нами рекомендации, как сказал Трипти, окажутся информативными и конструктивными. И второй комментарий, подготовкой которого мы занимаемся, содержит наши мысли о процессе в целом. Он будет передан в OEC.

КАВЕ РАНДЖБАР: Халед, вам слово.

ХАЛЕД КУБАА (KHALED KOUBAA): Спасибо. Хочу сообщить вам, что OEC сегодня утром, в 7:30, действительно провел неформальное обсуждение. Все его члены здесь также присутствуют. И мы подтвердили увеличение потока комментариев от сообщества на тему проверок. Мы также принимаем к сведению то, что многие группы интересов не удовлетворены проверками, их процедурой и способом их проведения. Поэтому наверняка будут приняты различные меры. Как сказал Йоран, будут

приняты краткосрочные, среднесрочные и долгосрочные меры.

Пока мы не сможем как OEC обсудить этот вопрос, потому что должны дождаться конца конференции, осмыслить все поступающие от сообщества комментарии и отзывы, а затем дать возможность корпорации ICANN систематизировать все эти комментарии и принять обоснованное решение на основе фактических данных, которое позволит OEC представить Правлению свои рекомендации.

Мы будем очень активно этим заниматься, так как поняли щекотливость этой проблемы и то, насколько важно сообществу проводить проверки наилучшим способом. И опять-таки я хочу сказать, что в долгосрочном плане также нужно задать вопрос о влиянии? Какое влияние оказывают эти проверки на нашу организацию? Но это вопрос, на который тоже следует ответить в долгосрочной перспективе. Спасибо.

КАВЕ РАНДЖБАР: Большое спасибо, Халед.

Есть еще вопросы? Шерин, прошу вас.

ШЕРИН ШАЛАБИ: Это не о проверках. Если есть минутка, я хотел бы обсудить рекомендации по развитию системы услуг корневой зоны.

КАВЕ РАНДЖБАР: Пожалуйста.

ШЕРИН ШАЛАБИ: Сейчас?

КАВЕ РАНДЖБАР: Да.

ШЕРИН ШАЛАБИ: Хорошо. Итак, по моему мнению, проблема связана с затратами.

Не знаю, сможете ли вы примерно оценить затраты на выполнение ваших рекомендаций, или над этим нам нужно поработать совместно. Поскольку, в настоящее время происходит следующее... и это наблюдается практически повсеместно... все группы заинтересованных сторон, которые... этим утром, например, мы встречались с SSAC.

И они говорят, что не в состоянии справиться с тем объемом работы, который необходим для выполнения

рекомендаций. Есть проблема затрат. Есть проблема ресурсов.

И мы, Правление, просто даем обратный ход. Для реализации рекомендаций, которые к нам поступают, необходимы затраты.

В этом конкретном случае, потому что это крайне важно, вы могли бы сообщить нам примерные затраты? Или нам нужно вместе поработать над этим?

ТРИПТИ СИНХА: По-моему, что касается затрат, в данном случае есть два вопроса. Один из них — это издержки на подготовку рекомендаций... в нашем случае, в консультативном комитете. И должна сказать, что меня озадачил объем работы, времени и участия, которые потребовались за последние три года.

И с этим объемом работы не связаны никакие расходы. Когда мы даем рекомендацию, безусловно, ее следует выполнить, то есть будут расходы непосредственно на реализацию. Именно на реализацию. Кроме того, есть другие расходы — это расходы на модель. После внедрения рабочей модели необходимо управлять новой инфраструктурой и заниматься ее обслуживанием. Да, это будет новая модель системы корневых серверов, какой бы она ни стала. Конечно, ее внедрение связано со значительными расходами для заинтересованных сторон

и так далее. Таким образом, мы на самом деле ведем речь о трех различных категориях затрат.

Так вот, собираемся ли мы указать в составе своих рекомендаций какие-либо суммы? Не в этой версии. Мы этого не планировали. Однако мы... по нашему пониманию, целесообразный алгоритм этой работы следующий: мы передадим рекомендации, Правление их обдумает и возможно обратится к нам с вопросами и просьбой глубже проанализировать, скажем, финансовые аспекты. Попросит глубже проанализировать то или иное, чтобы вы... тогда мы выполним более подробный анализ и глубже рассмотрим эти проблемы, а затем в определенный момент будет принято решение выполнить рекомендацию или не выполнять ее. И, как я уже сказала, реализация сопряжена с затратами, а если рекомендация будет выполнена, то потом потребуются расходы непосредственно на саму модель.

БРЭД ВЕРД: Да. И, пожалуй, только что описанный Трипти процесс обратной связи распространяется и на Правление, и на сообщество.

ШЕРИН ШАЛАБИ: Хорошо. Еще один вопрос на эту тему, потому что она важна. Итак, это влияет на системы корневых серверов и, следовательно, на операторов корневых серверов. Эти

рекомендации будут согласованными рекомендациями всех операторов корневых серверов или это будут только рекомендации RSSAC без полного консенсуса и согласия всех операторов?

ТРИПТИ СИНХА: Нет, консенсус будет, конечно, в пределах RSSAC, и мы предельно ясно заявили, что каждый из RSO, входящих в состав RSSAC, должен передать эту информацию своим компаниям-учредителям, чтобы до окончательного одобрения нами этих рекомендаций была получена информация о том, что все RSO согласны и поддерживают эту модель. Так что да, конечно, будет достигнут консенсус.

Мы полагаем, что эта проблема выходит далеко за рамки RSSAC и движущей силой процесса реализации станет все сообщество. Поскольку в состав этой модели вошло много компонентов, находящихся вне нашей компетенции.

КАВЕ РАНДЖБАР: Большое спасибо, Трипти. Хорошо. У членов Правления или RSSAC есть другие комментарии или вопросы на эту тему? Хорошо. Так как я не вижу желающих высказаться... для протокола хочу сказать, что уже после переклички к нам присоединились другие члены

Правления ICANN, Маартен, Лаусевиес, Лито, Рон, и Сара и Мэтью, а также Халед. И Леон. О, да. Извините.

Хорошо, переходим ко второму вопросу. Правление спрашивает RSSAC, какие важные цели RSSAC носят наиболее долгосрочный характер. Хочу пояснить. Главная причина этого вопроса в том, что Правление работает над следующим пятилетним стратегическим планом, поэтому мы хотим получить от RSSAC и наших групп интересов комментарии, по сути, чтобы учесть их в составе этого стратегического плана. Так что для нас это действительно крайне важный вопрос. Я знаю, что его обсуждение также продолжится в Панаме, но может быть у RSSAC на данный момент есть какие-либо комментарии. Брэд, Трипти.

БРЭД ВЕРД: Ну, по-моему, мы уже затронули это. Думаю, самыми долгосрочными нашими целями была бы реализация рекомендаций, которые мы дадим на ICANN 62. Очевидно, состоится, знаете ли... мы ожидаем, что состоится обмен мнениями между Правлением, а также в гораздо более широком масштабе с сообществом. Это начало диалога.

КАВЕ РАНДЖБАР: Большое спасибо. И как сказал во вступительном слове Шерин, я думаю также, что это уже включено в состав

ближайших приоритетных задач Правления, правильно, Шерин? Хорошо. Тогда позвольте перейти к следующему слайду? Следующий слайд. Да.

Это вопросы RSSAC Правлению. Я начну с первого: что вызывает озабоченность у Правления в связи с услугами корневой зоны... ощущает ли Правление давление, которое наблюдает RSSAC в отношении корневых серверов. Рам.

РАМ МОХАН: Спасибо. Рам Мохан. В связи с системой корневых серверов наибольшую озабоченность у Правления вызывает угроза атак DDoS, способных нарушить работу всей системы. Конечно же, эта угроза затрагивает не только систему корневых серверов. Все сервисы интернета находятся в опасности. Правление продолжает обсуждать возможные действия корпорации ICANN по смягчению этой угрозы. К сожалению, у корпорации ICANN мало возможностей в плане конкретных мер, способных оказать быстрое и прямое влияние на угрозу.

По-видимому, наиболее очевидной краткосрочной мерой является увеличение мощности корневых серверов, но это сопряжено с затратами и, конечно, с ограничениями по времени. Намерены ли операторы корневых операторов повышать их мощность, имеются ли у них

необходимые для этого ресурсы, финансы, персонал и так далее. Эти вопросы члены Правления обсуждали на внутренних совещаниях. Правление также заинтересовано в повышении общей подотчетности операторов корневых серверов.

Что касается ощущаемого Правлением давления на систему корневых серверов, Правление ощущает потребность в появлении новых операторов корневых серверов, не связанную с техническим аспектами. Правление знает, что сама корпорация ICANN должна принять все разумные меры для снижения угрозы атак DDoS. И наконец, Правление знает о требовании сообщества повысить подотчетность операторов корневых серверов и признает это требование справедливым. Именно эти вопросы были основными при обсуждении данной темы в Правлении.

КАВЕ РАНДЖБАР: Большое спасибо. Хочу вкратце рассказать вам предысторию. На наших открытых заседаниях с OCTO мы получили от OCTO предложения или возможные решения корпорации ICANN, направленные на смягчение части этих проблем. Кроме того, немного обсуждались дальнейшие шаги, и предложение OCTO было официально передано техническому комитету Правления. На следующем совещании технического комитета Правления, которое, по-моему, состоится на

следующей неделе, мы обсудим, как можно продвинуться вперед. Полагаю, что контакты с RSSAC и SSAC — одна из составляющих этого процесса. И эта дискуссия будет продолжаться.

Тем временем, по-моему, RSSAC уже проявил к этим предложениям интерес, состоялось их обсуждение, и некоторые высказались в их поддержку, а также было поднято несколько проблем. И я хотел бы попросить Брэда начать.

БРЭД ВЕРД: Да, я собираюсь затронуть ряд поднятых вопросов и оставлю вопрос DDoS напоследок, так как мне кажется, что диалог на эту тему будет более интенсивным. Что касается вопроса о подотчетности, поступившего от Правления и сообщества, как уже было сказано, мы работаем над ним и собираемся рассмотреть его в составе будущих рекомендаций Правлению. Я с неохотой вынужден сказать «ждите новостей», но мы потратили на это много времени. И мы стремимся изучить все ловушки и проблемы и ничего не упустить в своей модели. Для этого требуется время.

Что касается потребности нетехнического характера, не думаю, что она будет отдельно рассматриваться при определении концепции развития, но у Правления будут инструменты для реализации вписывающихся в эту

концепцию решений, которые оно сочтет целесообразными. Это политическая проблема, и есть технический комитет, чтобы давать рекомендации Правлению. То есть это что-то вроде «серой зоны».

Мощности... извините, мощности корневых серверов. Пожалуй, я могу просто указать на текущие темпы развития платформы, которая обслуживает корневую зону. Хочу сказать, что недавно, около года назад или чуть больше во всем мире насчитывалось 600 зеркал. На сегодняшний день в мире свыше 950 зеркал корневых серверов. Таким образом, их количество неуклонно растет. И это, как вы правильно отметили, одна из первых линий защиты от DDoS... риска DDoS. Думаю, что деятельность OCTO, связанная с корневым сервером L, информация о которой была получена Правлением и RSSAC, полностью соответствует тому, что сегодня делают другие операторы корневых серверов. Поэтому все наблюдаемые изменения в инфраструктуре конкретного сервера L происходят и в инфраструктуре сервера, обозначенного любой дугой буквой. Аналогичные действия предпринимают все операторы.

Что касается DDoS, угрозы сохраняются. Это не новая угроза для системы корневых серверов. Это существующая угроза, о которой RSSAC известно. Операторы корневых серверов обеспокоены. Это можно заметить по темпам расширения и количеству денег,

инвестируемых каждым оператором в расширение своей платформы. Я согласен с вами, что эта угроза не носит конкретного характера. Любой, кто подключен к интернету, находится в зоне риска. По-моему, во время нашей дискуссии с OCTO ранее на этой неделе был высказан интересный вопрос или соображение: «Корневая зона находится в опасности, как и любая другая платформа!». Пожалуй, есть TLD с такой же степенью риска, на которые может быть оказано огромное влияние через более короткий промежуток времени. Состоялась активная дискуссия на эту тему, которую следует принять во внимание.

Пожалуй, я коснулся всех вопросов. Если я что-то упустил, скажите, и я постараюсь к этому вернуться, или кто-то другой.

ХАЛЕД КУБАА: Спасибо, Брэд. Шерин?

ШЕРИН ШАЛАБИ: В связи с поднятым нами вопросом возникает еще один вопрос: почему сейчас? И позвольте мне это объяснять. Возможно для ответа мне понадобится ваша помощь. Итак, наша миссия всегда состояла в том, чтобы обеспечивать стабильную и безопасную работу системы идентификаторов интернета. Службы корневых серверов в прошлом, с первых дней существования ICANN,

работали весьма стабильно, верно? И продолжают работать. Поэтому я считаю, что мы должны попросить RSSAC объяснить, почему сейчас мы внезапно поднимаем эту проблему, правильно? Я хочу сказать, это до сих пор система работала стабильно. Безусловно, мы обязаны обеспечивать такую стабильность — это наша миссия. У нас нет прямой власти над операторами корневых серверов или возможности сделать что-либо еще. Почему сейчас эта проблема стала столь важна? Рам, возможно, вы объясните, какие наблюдаемые изменения в технологиях делают этот вопрос актуальным, как никогда раньше.

РАМ МОХАН: Спасибо, Шерин. Правлении это обсудило, и мы признаем и понимаем, что угроза атак DDoS не нова. Однако внимание Правления к этой проблеме возросло в связи с тем, что сейчас атаки имеют терабитный масштаб, который продолжает расти, и возникает впечатление, что темпы этого роста намного превышают темпы роста всех имеющихся мощностей. И опять-таки, мы признаем, что это относится не только к корневой системе. Не только к системе корневых серверов.

Вторым аспектом, усиливающим это беспокойство, является быстрый рост числа постоянно подключенных к интернету устройств, которые содержат встроенные уязвимости. Для создания из таких устройств сетей

зараженных машин требуется гораздо меньше усилий, чем раньше. Это усугубляется наличием систем с открытым исходным кодом, которые позволяют объединять такие устройства в огромную сеть атакующих устройств, способную нарушить работу всей системы. То есть дело не в том, что DDoS — неизвестный вид атак. Дело в том, что темпы роста мощности этих атак, кажется, намного опережают традиционные методы реагирования, которые обычно заключаются в наращивании мощностей и увеличении, знаете ли, пропускной способности, увеличении количества оборудования.

КАВЕ РАНДЖБАР: Позвольте мне начать этот диалог. Я вижу, что здесь присутствуют представители шести операторов корневых серверов из 12 организаций. Поэтому я могу задать вопрос, адресованный всем нам — операторам корневых серверов?

Кого-то из нас эти угрозы лишают сна? Поскольку я думаю, что в техническом отношении все мы понимаем размах и возможность этих угроз системе корневых серверов. Но кто-нибудь из нас лишился из-за этого сна? Или мы чувствуем, что небо падает на нас, и необходимо... пожалуйста.

ДЖЕФФ ОСБОРН (JEFF OSBORN): Джефф Осборн из ISC. Мы — оператор корневого сервера F. И одной из сильных сторон работы корневого сервера является разнообразие методов. Таким образом, все мы являемся разными организациями, которые выполняют свою работу по-разному. И их сочетание, по-моему, придает огромную силу.

ISC — стойкий приверженец интернета. Наша организация существует целую вечность. Стаж большинства моих сотрудников превышает десять лет. Совокупный опыт четырех членов правления составляет сотни лет работы в интернете. Это крепкая организация.

И за последние два с половиной года мы увеличили пропускную способность буквально больше чем на порядок, сначала обновив все наши аппаратные средства на местах и, во-вторых, в партнерстве с CloudFlare, провайдером огромной пропускной способности, в значительной степени во всем мире. Две недели назад я был в Катманду, когда мы устанавливали там зеркало корневого сервера F.

И без преувеличений можно сказать, что те объемы данных, которых мы сейчас боимся, не заставят оборудование CloudFlare отключиться. Таким образом, вместо ситуации, когда длительная атака гигабитного масштаба была заметна и вызывала озабоченность, мы

оказались в ситуации, когда это просто одна из записей в журнале. Это вообще не проблема.

Я видел в отчете OCTO, что ICANN как оператор корневого сервера, похоже, не пойдет таким путем. По-моему, это здорово. По-моему, просто прекрасно, что по этому вопросу у нас есть расхождение во мнениях.

И хочу подкинуть сумасшедшую идею о журавле в небе. Моему правлению нравится идея разместить десять тысяч крошечных устройств Anycast в разных точках мира, чтобы были перехватывающие устройства, которые настолько малы, что никакая атака DDoS не сможет получить развития, потому что все будут поглощать эти «жертвенные» узлы, рассеянные по всему миру.

Сила DDoS в том, что огромное количество устройств объединяется для поражения одной цели. И природа Anycast приведет к тому, что вместо этого атака будет поглощена локальным зеркалом.

Таким образом, мы достаточно много размышляем об этом. Но я не лишаюсь сна по этому поводу. Думаю, что мы движемся в интересном направлении.

И последнее, что я хочу сказать. Если мы начнем здесь хвастаться тем, насколько хорошо мы защищены от атак, то нам сразу же начнут звонить технические сотрудники наших организаций, сообщая, что эти заявления послужили причиной атаки. По существу, мы должны

проявлять скромность, чтобы не получать таких неприятных сообщений.

КАВЕ РАНДЖБАР: Большое спасибо.

Выступает Лиман, затем Рам, а потом Давид.

ЛАРС-ЙОХАН ЛИМАН: Ларс Лиман из Netnod. Мы тоже управляем одним из зеркал.

Я хотел бы добавить ко всему сказанному, что внедряются и другие защитные механизмы. И они относятся к фильтрации, к взаимоотношениям между операторами корневых серверов и различными интернет-провайдерами, которые не по своей воле являются распространителями атак, в нашем случае, на корневые серверы.

Есть целая сеть людей и организаций с добрыми намерениями, желающих сохранить работоспособность систем. И это действительно очень важный ресурс. Таким образом, мы не одни. Есть целый интернет, который стремится помочь нам.

Спасибо.

КАВЕ РАНДЖБАР: Большое спасибо.

Рам.

РАМ МОХАН: Спасибо. Я хочу вернуться к чему-то, что было сказано. Видите ли, в отчете OCTO говорится о том, что методы расширения корневого сервера L — увеличение количества зеркал L, кластеры L, отдельные зеркала L и так далее — все эти способы расширения можно применить ко всем другим буквам.

Правлению неясно, является ли это тем же самым видом инвестиций или тем же самым направлением при планировании наращивания мощностей, которое сейчас идет. Речь не идет о том, что этого не происходит. Речь идет об отсутствии понимания.

У нас также вызывает обеспокоенность то, что вместо атак, знаете ли, имеющих масштаб 1,7 терабит в секунду, мы можем столкнуться с атаками, имеющими масштаб 5, 7, 10 терабит.

И мы хотели бы понять: Идет ли процесс соответствующего планирования? Осуществляется ли надлежащее управление рисками? Какие механизмы борьбы имеются у тех, кому доверено управление системой корневых серверов?

Думаю, что такой уровень диалога и обучения Правления принесет огромную пользу в деле смягчения некоторых существующих проблем.

Еще одной вещью, которая могла бы принести пользу и способствовать подотчетности, это подготовка обобщенного отчета, где были бы отражены инвестиции или расширение мощностей и тому подобное. Возможно, на некотором унифицированном метауровне, позволяющем опубликовать эти данные для сообщества, потому что об этом просит не только Правление. Такие просьбы также поступают и от членов сообщества. Спасибо.

КАВЕ РАНДЖБАР: Давид, вы хотите ответить? Кто-нибудь хочет ответить на эти вопросы. Да, если вы хотите ответить, пожалуйста.

БРЭД ВЕРД: Есть несколько соображений. Во-первых, я хочу указать, что этот ряд вопросов действительно имеет операционный и обоснованный характер, но RSSAC не обязательно отвечает за RSSAC. Как уже было указано, за пределами сервера L отсутствует какая-либо операционная подотчетность.

Поэтому я считаю... я не хочу упускать из виду тот факт, что мы продолжаем заниматься развитием системы.

Наша цель в том, чтобы предусмотреть в составе той модели аспекты организационного управления и операционной подотчетности. Так вот, я знаю, что этот вопрос будет решен и не терпит отлагательства — существует риск, который заставляет задавать эти операционные вопросы. Мы понимаем, что в общем-то есть неотложная потребность и, если это имеет смыл, в дальнейшем будет подготовлен отчет. Я не хочу упускать это из виду.

Честно говоря, как оператор корневого сервера, а не как представитель RSSAC, я думаю, что это... я не знаю, как отнеслась бы моя организация к составлению метаотчета, в котором отражены наши мощности и инвестиции, потому что не хотелось бы давать в руки злоумышленникам дорожную карту с описанием инфраструктуры. Это очень важный момент. И об этом следует помнить при обсуждении данной темы.

Не хочется публиковать точные данные о пропускной способности системы. Нет никакого желания публиковать какие-либо количественные показатели. Это следует учитывать на операционном уровне, не на уровне политики, но на операционном уровне. Это риск, который должны учитывать Правление, сообщество, люди, которые спрашивают, насколько сильно меняется ситуация. Целесообразно ли это делать.

РАМ МОХАН: Очень кратко, Каве.

Брэд, я думаю, что Правление целиком с вами согласно. Есть полное понимание того, что нежелательно давать в руки злоумышленникам дорожную карту, позволяющую найти уязвимости и атаковать.

Помимо прочего, нам нужно совместно проработать следующий вопрос, который, как я очень хорошо помню, поднимался во время одной из дискуссий на семинаре Правления: Давайте представим, что произошла серьезная атака, после которой, знаете ли, часть корневой системы потеряла работоспособность. Кто сообщит об этом некоторому комитету? И какой вопрос тогда будет задан? А будет задан следующий вопрос: Вы знали, что может возникнуть такая угроза? Вы знали, что была существенная угроза, в результате которой часть системы, считающейся ядром интернета, могла потерять работоспособность. Какие меры вы приняли?

Таким образом, я думаю, что мы пытаемся просто наладить сотрудничество, чтобы получить общие и конкретные ответы, не забывая о том, что ни у кого нет желания раскрывать все операционные подробности. Это важная работа. Это полезная работа. Мы не хотим о ней рассказывать. Но в то же время, я думаю, что Правление хочет повысить прозрачность и обрести определенную степень уверенности в том, что такая

работа идет, а не только слышать слова: «верьте нам, что это происходит», правильно?

По-моему, именно это сейчас происходит. Извините за откровенность. Но я считаю, что именно таков реальный характер этой дискуссии в Правлении.

КАВЕ РАНДЖБАР: Спасибо. Кто-нибудь желает ответить? Трипти, пожалуйста.

ТРИПТИ СИНХА: Итак, Рам, у меня есть двойной ответ на ваш вопрос. Во-первых, мы полностью понимаем позицию Правления, что вам требуется описание нашей работы. И мы уважительно к ней относимся. Мы это понимаем. Угрозы всегда существовали, будь то угроза применения ядерного оружия, угроза вооруженного конфликта или киберугроза. Мы отслеживаем такие угрозы и продолжаем улучшать свою работу по мере возможности. И я понимаю, что нам нужно передать вам какой-то обобщенный отчет и сообщить, что делают операторы корневых серверов в совокупности. Я полностью согласна с Брэдом. Мы не хотим раскрывать детали своей работы, но можем, конечно, составить некий обобщенный отчет и убедить вас, что ситуация находится под контролем. И мы контролируем ее уже не один десяток

лет. Это относится не только к системам корневых серверов. Это относится к любым видам угроз.

Так вот, мы продолжаем работать над своими рекомендациями, так как понимаем, что нам нужна подотчетность. Кто наши заинтересованные стороны? Все мы — вымирающий вид. Мы были здесь с момента создания системы корневых серверов. В один прекрасный день мы исчезнем. Мы должны передать это кому-то и создать новую модель. Именно это побуждает нас делать то, чем мы сейчас занимаемся. Но параллельно мы продолжаем укреплять свои службы. Мы делаем это по-разному. Мы — это 12 различных организаций. Огромное разнообразие. В общем, я не знаю, ответила ли на ваш вопрос.

КАВЕ РАНДЖБАР: Я спросил у Давида, можем ли мы продолжить обсуждение этого вопроса, прежде чем он выступит со своими комментариями. И мы можем потратить на эту тему еще десять минут.

РАМ МОХАН: Буду очень краток. Не думаю, что нам удастся решить этот вопрос сейчас, но это начало действительно полезного диалога. И нам нужно... и я буду говорить от своего имени. Не от имени Правления.

Лично я считаю, что нам нужен механизм, позволяющий постоянно поддерживать этот диалог, не только на заседаниях, но и между ними, потому что, как вы указали, нам известно об этих угрозах, а также о других угроза, верно? И, по-моему, нам нужен пока еще не существующий механизм, позволяющий не прерывать этот цикл обсуждения.

Лично я очень хочу найти способ сделать это, потому что он позволит собраться вместе, чтобы сказать вам: «Эй, нас волнует не только операционная часть, но также и то обстоятельство, чтобы, когда что-то действительно происходит с операционными функциями, ваши слова заслуживали доверия и подкреплялись фактами»? Знаете ли, это можно сделать только в том случае, если постоянно вести диалог.

БРЭД ВЕРД: Единственное, что я добавлю и буду очень краток. Это касается вашего комментария насчет 1,7 гигабит. Что впоследствии будет 5 и 6 терабит. По-моему, пять или шесть лет назад мы обсуждали, что произойдет в случае атаки, масштаб которой составит один терабит, как мы планируем к ней подготовиться и как мы собираемся справиться с подобной ситуацией.

Я думаю, что это нормальный процесс перетягивания каната между хорошими парнями и злоумышленниками,

согласны? Они делают шаг вперед, мы реагируем. Векторы атак постоянно меняются. Не существует универсального решения всех проблем. Вы постоянно добавляете новые инструменты в свой комплект инструментов для противодействия злоумышленникам.

КАВЕ РАНДЖБАР: Большое спасибо. Другие вопросы или комментарии на эту тему? Да, пожалуйста.

РАМ МОХАН: Буду краток, и я вижу, что Лито тоже здесь присутствует. Лито и я — сопредседатели Комитета Правления по оценке риска.

Принципиально важной вещью, которую мы рассматриваем, по-моему, является подход к управлению рисками, верно? Речь идет не о том, чтобы знать все решения, а о том, чтобы понимать, что риски и меры борьбы с ними были продуманы. Тогда возникает обоснованная уверенность в том, что эти меры могут оказаться успешными.

КАВЕ РАНДЖБАР: Хорошо. Если больше нет комментариев, Давид, вам слово.

ДАВИД КОНРАД: Да, я только хотел пояснить один момент. В отчете перед Правлением, который OCTO передал Правлению и впоследствии RSSAC, перечислен ряд возможностей, которые организация рассматривает в контексте работы корневого сервера L, а также возможностей по защите услуг корневой зоны. Там не указано, что принято конкретное решение о целесообразности использования какого-то определенного подхода.

Мы действительно представили ряд предложений, которые, по мнению OCTO, соответствуют рациональным подходам, но некоторые из предложенных в документе вариантов потребовали бы очень большого количества ресурсов.

Так что, как ни хотелось бы мне иметь возможность диктовать, на что следует потратить деньги, это вне моей компетенции.

КАВЕ РАНДЖБАР: Большое спасибо.

Давайте перейдем к следующей теме? Если есть комментарии или вопросы, я готов... хорошо.

Второй вопрос RSSAC Правлению относится к мнению Правления о предложенном плане обновления KSK. И для ответа на него... по существу Правление поручило Давиду ответить на вопрос об обновлении KSK.

Давид.

ДАВИД КОНРАД: Текущая ситуация такова. У нас есть данные, которые позволяют предположить, что после обновления KSK некоторый процент резолверов будет неправильно сконфигурирован, что приведет к ошибкам при разрешении доменных имен, если включена проверка подлинности DNSSEC. Однако эти данные приносят мало реальной пользы, потому что проект обновления KSK изначально учитывал возможность воздействия на пользователей. Согласно положениям этого документа, обновление KSK может оказать отрицательное воздействие не более чем на 0,5% пользователей. Если бы это произошло, то мы отказались бы от обновления.

Сейчас мы стараемся провести дополнительное общественное обсуждение предложенного плана перенести дату обновления на 11 октября 2018 года, независимо от данных, которые мы получаем и которые известны как 8145 отчетов резолверов.

Таким образом, наверное, вопрос отчасти в том, какое мнение у RSSAC о предложенном плане и что RSSAC предложил бы сделать для смягчения рисков и проблем, связанных с обновлением.

КАВЕ РАНДЖБАР: Еще раз повторю то, что было сказано на совещании с OCTO. Как было указано на графике, в мае... вполне возможно, что в мае Правление примет резолюцию и попросит RSSAC и SSAC дать рекомендации, поскольку такова процедура. Придется предпринять несколько шагов, прежде чем Правление сможет принять указанную резолюцию. Тем временем, ничто не мешает SSAC или RSSAC начать работу над своими рекомендациями или, если у них уже есть какие-либо комментарии, дать рекомендации. Прошу вас иметь это в виду и запланировать соответствующую работу, если она необходима.

Большое спасибо.

Что касается последнего вопроса, по сути он относится к срокам. Поскольку вопрос поступил, и в то же время возникла проблема с рекомендациями, я попрошу Брэда дать пояснения.

БРЭД ВЕРД: Да. Думаю, что этот вопрос потерял актуальность в связи с произошедшими событиями. Этот вопрос был в общем-то реакцией на вопрос GNSO, предложившей различным AC прокомментировать добавление до 25 000 к пространству имен.

Учитывая что RSSAC и SSAC уже ответили, и этот вопрос Правлению был составлен задолго до того, как это было сделано.

Если вы не хотите добавить что-то новое от имени Правления, то я думаю, что этот вопрос потерял свою актуальность.

КАВЕ РАНДЖБАР: Большое спасибо, Брад.

Есть дополнительные комментарии на эту тему?

Хорошо. Если нет, то может быть кто-то из членов Правления или RSSAC хочет вынести на обсуждение другую тему?

Или, поскольку у нас осталось немного времени, кто-то из присутствующих в зале заседаний, хотя на это совещание были допущены в основном наблюдатели. Но если у кого-то есть содержательный комментарий, касающийся RSSAC или взаимоотношений Правления с RSSAC, я с огромной радостью предоставлю вам слово.

Хорошо. Так как никто не проявил желания, мы закрываем это заседание.

Спасибо, что присоединились к нам. Пока!

[КОНЕЦ СТЕНОГРАММЫ]