ICANN76 | CF– Программа ICANN Fellowship: вводный курс по ICANN OCTO и KINDNS
Воскресенье, 12 марта 2023 года – с 10:30 до 12:00 по CUN

СИРАНУШ ВАРДАНЯН: Всем привет и добро пожаловать на второй день ICANN76. Надеюсь, что вчера всем понравилось. Меня зовут Сирануш Варданян, и я приветствую всех вас на заседании с участием нашей технической команды и команды IANA. Они расскажут подробнее обо всех этих аббревиатурах.

Но перед этим небольшое объявление. Я буду вашим менеджером дистанционного участия на этом заседании, и это заседание будет записываться и регулироваться в соответствии со стандартами ожидаемого поведения ICANN.

Во время этого заседания вопросы и комментарии, отправленные в чате, будут зачитываться только в том случае, если они будут правильно оформлены, как отмечено в чате. Если вы захотите выступить во время заседания, поднимите руку, и, когда к вам обратятся, виртуальные участники включат свои микрофоны в Zoom. Очные участники будут пользоваться физическими микрофонами. У нас здесь два передвижных микрофона. Для удобства других участников называйте для протокола свое имя и не говорите слишком быстро.

У нас есть устный перевод на шесть языков ООН, и я призываю всех, прежде чем садиться, взять другие наушники и

воспользоваться устным переводом. У нас отличная команда переводчиков.

Итак, я хотела бы представить наших сегодняшних докладчиков, и начну с технического директора Джона Крейна, который находится здесь со своей командой, Дэвидом и Ким Дэйвис, которые представят тему и расскажут об IANA. Но начнем мы с Джона. Джон, вам слово.

ДЖОН КРЕЙН: Большое спасибо. Рад видеть вас всех здесь. Как известно Сирануш, Fellowship и NextGen — мои любимые группы в ICANN, потому что вы все — свежие лица со свежими идеями и т. д. Поэтому мне всегда приятно быть здесь. Я Джон Крейн. Я старший вице-президент и технический директор ICANN. Я работаю в ICANN уже несколько десятилетий или даже больше. Прошло немало времени. Я, так сказать, часть мебели.

Я руковожу группой, которая называется IROS. Неспециалисты нечасто о ней слышат. Это в значительной степени наша внутренняя группа. Эта группа занимается аббревиатурами. Мы обожаем аббревиатуры. IROS — это функциональная группа по изучению, эксплуатации и обеспечению безопасности идентификаторов. Так что это касается доменных имен, IP-адресов, всех [избыточных] идентификаторов. Буква "I" в начале очень важна. Мы вплотную занимаемся идентификаторами и тем, что с ними происходит.

И можно разделить это на три модуля. У нас есть группа под названием IANA (Администрация адресного пространства Интернет), которой руководит этот джентльмен слева от меня, Ким Дэйвис. Затем у нас есть группа, которая в значительной степени сосредоточена на взаимодействии по техническим вопросам, ей руководит мой друг Адиэль, а справа от меня находится Дэвид. А затем много исследований. Над этим работают два моих менеджера. Я вижу, что один из них очень застенчив и прячется среди участников. Привет, Саманех. Почему бы тебе... Ты даже можешь присоединиться к нам, если хочешь. И я не вижу Мэтта, но я знаю... Мэтт там. Мэтт тоже может прийти и присоединиться к нам, если мы захотим, или он может просто застесняться и остаться там. Вам решать.

Это то, чем мы занимаемся. Мы проводим исследования по всем вопросам, затрагивающим идентификаторы. Цепочка IANA управляет многими из этих идентификаторов с операционной точки зрения. А потом мы выходим и говорим об этих вещах.

Я не хочу тратить наше время на поучения, поэтому я дам некоторым из этих ребят немного времени, чтобы рассказать о том, над чем они работают. И я собираюсь начать с того, что, возможно, является самым важным в работе ICANN, потому что вы собрались здесь на конференцию по вопросам политики, но политика важна только в том случае, если вы можете ввести ее в действие и реально управлять этими идентификаторами. Так что я передам слово Ким, если хотите. Почему бы вам не рассказать нам немного о роли IANA?

КИМ ДЭЙВИС: Я буду краток, потому что у меня в общем-то есть презентация, но я расскажу вкратце. Роль IANA заключается в том, чтобы быть центральным информационным депозитарием, хранилищем записей для всех идентификаторов, которые мы используем в Интернете. Я думаю, что большинство здесь знают о доменных именах. Обычно они чаще всего вспоминаются, когда мы говорим об интернет-идентификаторах, но ни в коем случае не являются единственными. IP-адреса вам, вероятно, тоже знакомы, но существуют буквально тысячи идентификаторов, используемых для обеспечения повседневной связи в Интернете, о которых вы, вероятно, не знаете. И для того, чтобы Интернет работал, необходимо некое централизованное место, где присваиваются эти идентификаторы, чтобы это делалось последовательно во всем мире. И вот это лежит в основе функции IANA. Об этом мы поговорим чуть позже, но вкратце это то, чем мы занимаемся.

ДЖОН КРЕЙН: Хорошо. Буква R означает исследование. Итак, Саманех или Мэтт, почему бы вам не рассказать немного об основах того, чем занимаются ваши группы.

САМАНЕХ ТАДЖАЛИ (SAMANEH TAJALI): Я Саманех Таджализадехуб, возглавляю исследовательскую группу по безопасности, стабильности и устойчивости (SSR) в Офисе технического

директора. Темы, которые мы рассматриваем, в основном косвенно или напрямую связаны с безопасностью DNS. Это могут быть некоторые из тем, которые вы часто слышите на конференциях ICANN, а именно: злоупотребление DNS, а также конфигурации безопасности DNS, все косвенные вещи, которые влияют на имена и которые также влияют на злоупотребление — такие вещи, как фишинг, вредоносное ПО, управление и контроль, веб-безопасность, безопасность протоколов и т. д.

Теперь я передам слово Мэтту.

МЭТТ ЛАРСОН (MATT LARSON): Я Мэтт Ларсон. Я также руковожу исследовательской группой. Иногда мы занимаемся безопасностью, но не всегда уделяем ей такое внимание, как команда Саманеха. Мы много работаем. У нас есть несколько больших массивов данных, с которыми мы работаем. Нам очень повезло, что мы имеем доступ к трафику корневого сервера под управлением ICANN. Поэтому мы проводим исследования, основываясь на нем. Мы также проводим исследования, основанные только на содержимом DNS. У нас есть доступ ко всем файлам корневых зон gTLD и некоторым файлам корневых зон ccTLD. Таким образом, это очень богатые наборы данных, с которыми можно работать. Мы также активно работаем в области стандартов, в частности в IETF. То есть мы составляем протоколы разъяснений и усовершенствований, а также документы, связанные с операционной деятельностью.

ДЖОН КРЕЙН: Дэвид, почему бы вам не рассказать немного о работе по вовлечению?

ДЭВИД ХУБЕРМАН: Конечно. Привет! Доброе утро! Я Дэвид Хуберман, и я работаю в отделе, который мы называем «Взаимодействие с техническим сообществом». Мы — это штат инженеров со всего мира, которые работают как с техническими, так и нетехническими сообществами для создания хорошего потенциала и развития навыков в области DNSSEC, безопасной маршрутизации и в плане RPKI с RIR. Мы работаем над взаимодействием, особенно с нетехническими сообществами, по темам, связанным с ICANN, чтобы обеспечить хорошее, глубокое понимание инженерных разработок, лежащих в основе инфраструктуры Интернета, и того, как построен Интернет. И мы много сотрудничаем с друзьями и коллегами в ICANN, с правительствами и нетехническиими сообществами над тем, чтобы все говорили на одном языке о том, как работает Интернет.

ДЖОН КРЕЙН: Отличный обзор.

Я предлагаю перейти к вопросам через минуту, потому что вы уже достаточно о нас слышали, но перед этим, пожалуйста, встаньте сотрудники IROS в зале, чтобы люди знали, к кому идти и кого расспрашивать.

Хорошо. Здесь, на конференции ICANN, нас гораздо больше. Штат намного больше, чем сейчас присутствующие, но мы привозим на конференции ICANN небольшой контингент, чтобы мы могли взаимодействовать с сообществом и проводить здесь работу. Поэтому мне важно услышать вас.

Поэтому я возвращаю слово коллеге, и мы посмотрим, есть ли вопросы.

СИРАНУШ ВАРДАНЯН: Спасибо, Джон. Эта сессия запланирована специально для участников Программы Fellowship и NextGen, поэтому я призываю всех вас активно задавать вопросы, ведь это уникальная возможность для всех вас. Многие из вас являются техническими специалистами, но очень важно понимать, как с технической точки зрения работает ICANN. Поэтому, пожалуйста, не стесняйтесь. Как я уже говорил вам во время первой сессии, глупых вопросов не бывает. Поэтому, пожалуйста, задавайте вопросы, и мы можем начать прямо сейчас. Обо всем, что вас интересует. У нас есть микрофоны. Я могу попросить разместить здесь два микрофона? У нас они есть, я думаю. Итак, все желающие, поднимайте руку. Да, микрофоны сейчас будут. Дайте нам две секунды.

Да, пожалуйста. Вот сюда. Вы не могли бы взять микрофон? И начнем отсюда.

Николас, мы к тебе вернемся, да. Спасибо.

ХАРИШ ЧОУДХАРИ: Приветствую всех. Я Хариш Чоудхари, участник программы ICANN Fellowship. Я научный сотрудник в Национальном университете судебной экспертизы в Индии, и мои исследования посвящены безопасности DNS. Поэтому мой вопрос к исследовательской группе: как я могу внести свой вклад? Потому что я работаю именно над безопасностью ccTLD .in и связанными с этим показателями. Как я могу внести свой вклад в эту работу? Как я могу освоить новую технологию в команде, чтобы она помогла обеим сторонам? Спасибо.

ДЖОН КРЕЙН: Саманех, ответите на этот вопрос?

САМАНЕХ ТАДЖАЛИ (SAMANEH TAJALI): Да. Спасибо, Джон. Спасибо за вопрос. Рад видеть вас здесь, в зале. На самом деле, я точно знаю... Не знаю, знаете ли вы, ребята, о проекте DAAR в ICANN, который существует уже четыре года. Он называется «Платформа отчетности о случаях злоупотребления доменами». И .in является частью этого проекта. Таким образом, мы уже сотрудничаем с .in. Я хотел бы услышать от вас, над какими темами безопасности вы работаете, можете ли вы содействовать, можем ли мы работать вместе, можете ли вы предоставить полезные данные или рассказать об этом. Если нужно, укажите правильное направление. Но мы много работаем в области безопасности TLD,

поэтому должны быть области, в которые мы можем направить вас или быть полезными.

ДЖОН КРЕЙН: Да. Мы также публикуем много документов в серии, которую мы называем OCTO Series. Если вы увидите одну из них, и она будет интересной, и вы подумаете, что это хорошо, или вы подумаете, что это ужасно — надеюсь, такого не случится — напишите нам. Прокомментируйте. Пожалуйста, найдите время, чтобы поговорить с Саманехом или любым из членов команды. Мы всегда ищем людей, с которыми можно сотрудничать и выяснять, правильно ли мы проводим исследования или есть способы улучшить их.

СИРАНУШ ВАРДАНЯН: Спасибо. Николас, пожалуйста? Вы следующий.

НИКОЛАС ФУМАРЕЛЛИ: Приветствую команду OCTO в ICANN. Здесь я отметил, что защита маршрутизации не является частью миссии или целей ICANN, но вы недавно упомянули о RPKI и ее важности для защиты маршрутизации. Итак, вы можете прояснить, как безопасность маршрутизации сочетается с работой ICANN, если вообще сочетается?

Кроме того, если защита маршрутизации действительно является частью исследований ICANN, мне интересно, насколько устойчива

инфраструктура крупных компаний и популярных приложений. Например, несколько лет назад произошел инцидент с компанией Meta (ранее Facebook), связанный со сбоями DNS и BCP. Можете ли вы найти какие-либо сведения о том, как такие компании, как Meta, справляются с защитой маршрутизации и какие шаги они предпринимают для обеспечения устойчивости инфраструктуры? Спасибо за ваше время и понимание.

ДЖОН КРЕЙН: Тут очень много вопросов. Я попытаюсь разбить некоторые из них, и начну с простого, а именно: входит ли маршрутизация в компетенцию ICANN? ICANN — это не DNS. ICANN занимается идентификаторами. Если считать, что маршрутизация является для IP-адресов тем же, чем разрешение является для DNS, то, очевидно, мы заинтересованы в этом.

Когда мы имеем дело с DNS, нашими партнерами — поскольку ICANN является частью сообщества — как правило, являются регистратуры, регистраторы и поставщики разрешений. А в мире IP-адресации нашими партнерами в этих обсуждениях и исследованиях, как правило, являются RIR (региональные интернет-регистратуры), иногда провайдеры интернета и т. д.

Это область, отличная от DNS, но мы занимаемся не только DNS.

Позвольте мне передать слово Дэвиду, чтобы он немного рассказал о некоторых из этих вещей.

ДЭВИД ХУБЕРМАН: Здравствуйте. Это отличный вопрос, и это вопрос, который мы иногда обсуждаем и между собой, потому что мы не хотим выходить за рамки наших полномочий. Но правда в том, что RPKI и эта большая идея защиты маршрутизации, когда провайдеры услуг Интернета и все участники маршрутизации в Интернете передают трафик и передают объявления о том, кем они являются — «Эй, это моя сеть; это мои услуги; если вы хотите туда попасть, приходите ко мне через эти объявления о маршрутизации» — в течение 30 или 40 лет были очень небезопасными.

Теперь мы обеспечиваем их безопасность. Мы защищаем их с помощью инфраструктуры, которая, надеюсь, сможет предотвратить многие происшествия и многие злоупотребления, о которых вы иногда читаете. И как отрасль, мы, конечно, не хотим, чтобы вы читали об этом, потому что мы не хотим, чтобы это произошло, потому что мы хотим, чтобы базовая инфраструктура просто работала, чтобы, когда вы принимаете чей-то совет, вы могли перейти на любой нужный вам сайт, и это просто работает, и вам не нужно думать об этом. Таким образом, у нас есть этот слой безопасности, который мы создаем поверх этого, и мы должны быть уверены, что он сделан хорошо и правильно.

В то же время, мы должны осознавать, что вся инфраструктура имен и номеров, которая, конечно же, находится в нашей компетенции, находится за этой инфраструктурой безопасности, за этим уровнем безопасности. И если это сделано плохо, и мы не можем получить доступ к серверам имен и резолверам, если мы не можем получить доступ к различным компонентам, на которые мы

смотрим, это проблема, верно? Поэтому мы уделяем этому большое внимание.

Далее, вы спросили конкретно о Meta. Вы спрашивали о том, как в октябре 2021 года Facebook был полностью недоступен почти целый день. И причина была в DNS. В мире Интернета существует мем: если что-то ломается, то это вина DNS, потому что, и это примечательно, очень часто это происходит по вине DNS.

Здесь у Meta была очень интересная конфигурация, в которой физический доступ в здания, например, в центр обработки данных, в офис Facebook... Они использовали пропуска, как и любая другая корпорация, верно? Но вся система была привязана к системе DNS. И чтобы проверить подлинность вашей личности, они использовали DNS, чтобы найти хранилища, где была эта информация, верно? Но внутри произошел сбой. Внутри произошел сбой, который распространился каскадом и сделал DNS недоступным не только для всего мира, но и для всех систем внутри Meta. Это означало, что, когда вы входите в дверь, для проверки подлинности требовался DNS, чтобы найти вас. Но доступа к DNS не было. Это удивительно творческий способ сломать вещи.

И чему, как мне кажется, это научило не только Meta, но и всех остальных, так это тому, что при создании инфраструктуры, будь то корпоративные ИТ, будь то гигантская глобальная сеть, на которую полагаются многие и многие люди для доступа или получения контента, нужно действительно думать о

взаимодействии между маршрутизацией, авторизацией, аутентификацией и DNS. И не создавайте случайных отказов, которые могут привести к каскаду неудач и превратить вас в остров, с которого никто не может выбраться.

Так что это был очень интересный инцидент, и я думаю, что все многому научились.

ДЖОН КРЕЙН: И если вы оглядитесь, вы можете встретить здесь людей из Меты. Это была их сеть и их проблема, так что, возможно, стоит узнать их мнение по этому поводу.

СИРАНУШ ВАРДАНЯН: Спасибо. Для целей устного перевода, пожалуйста, говорите в разумном темпе.

У нас есть удаленный вопрос от Шанель Макферсон, участницу Программы NextGen на ICANN76. Пришлось перенести на последний момент, но ее вопрос для команды Джона Крейна. «Как происходит развертывание DNSSEC, и как местный интернет-провайдер может принять участие в его реализации?».

ДЖОН КРЕЙН: Итак, во-первых, Шанель, мне очень жаль, что вы не смогли приехать. Надеюсь, что мы встретимся где-нибудь в будущем. Надеюсь, вы будете продолжать подавать заявки на участие в конференции ICANN, и мы увидимся с вами в следующий раз.

Сначала я передам слово Киму, который расскажет о том, как это внедряется, а затем попрошу Дэвида рассказать немного о нашей работе, связанной с вовлечением в DNSSEC. Итак, Ким, почему бы вам не поговорить немного о корне?

КИМ ДЭЙВИС: Спасибо, Джон. Итак, одна из функций IANA, которую мы еще не обсуждали, — это управление корневой зоной DNS. Корневая зона DNS — это, пожалуй, самая важная часть DNS. Это первое место, куда обращаются компьютеры, имеющие доступ к DNS, чтобы найти адрес, который они ищут. В ней находится аутентичная запись о том, какие домены верхнего уровня существуют и где в Интернете находятся серверы, отвечающие за эти домены верхнего уровня.

В нашу зону ответственности за управление корневой зоной DNS входит управление криптографическими ключами, которые защищают корневую зону для DNSSEC. Это особенно важная часть нашей деятельности. На самом деле, у нас много ресурсов, выделенных только на эту функцию в рамках IANA. И причина этого проста. Работа DNSSEC заключается в наличии одного центрального ключа, с помощью которого запускают процесс поиска DNS. И очень важно, чтобы этот ключ хранился в очень безопасной форме и в надежных условиях, которые, по мнению сообщества, исключают риск несанкционированного доступа к этому ключу.

Поэтому мы делаем это так: мы храним этот ключ в безопасности. Это входит в наши обязанности. Мы храним его в нескольких очень хорошо защищенных помещениях. И каждые три месяца мы получаем доступ к этому ключу, чтобы использовать его на важных публичных мероприятиях, которые мы называем церемониями смены ключей. Мы привлекаем к этому сообщество. Мы ведем прямую трансляцию. Это очень публичное мероприятие. Но мы делаем это таким образом, чтобы эксперты по безопасности, в частности, могли наблюдать за тем, что мы делаем, и могли сказать: «Да, ICANN следовала хорошей процедуре, сделала это таким образом, что нет риска несанкционированного использования этого ключа». И все расходятся довольные.

И поэтому, как я уже сказал, это ключевая часть наших операционных процессов. Я могу целый час рассказывать о том, как они работают. Это очень интересная тема. Но это действительно одна из самых основных обязанностей по безопасности DNSSEC, которые несут IANA и ICANN.

Но я хочу отметить, что вопрос был о том, что такое ISP в контексте DNSSEC. Поэтому я передам вам микрофон, чтобы вы немного рассказали об этом.

ДЭВИД ХУБЕРМАН: Разумеется. После того как команда Кима проделала огромную работу по обеспечению работоспособности DNSSEC в корневой зоне, мы должны ее использовать. И как же мы ее используем? Что ж, переходим на следующий уровень, который является доменом

верхнего уровня: .com, .org, .museum. Или, в данном случае, я хотел бы сосредоточиться на кодах стран. Мы в Мексике: .mx. Итак, если мы хотим установить DNSSEC в Мексике для любого домена, относящегося к TLD .mx, мы обращаемся к оператору регистратуры .mx. И этот оператор регистратуры подписывает свою собственную зону и предлагает подписание и проверку DNSSEC каждому домену, находящемуся под ним.

Я смотрю на аудиторию и вижу своего коллегу Николаса Антониеллу. Николас, который находится в Уругвае в Южной Америке... И что делает Николас? Он посещает различных интернет-провайдеров и операторов регистратур национальных доменов верхнего уровня и работает с ними над установкой подписи DNSSEC, обучая их всему, что им нужно знать о том, как это работает, и, что очень важно, об инструментах, необходимых для поддержания этого. И он может работать с интернет-провайдерами, чтобы убедиться, что они проверяют на своих резолверах: когда домены подписаны DNSSEC, они могут проверить эти подписи и передать их дальше.

Поэтому ICANN работает на корневом уровне, чтобы гарантировать, что все подписано, и убедиться, что все может быть подтверждено ключами. И еще ICANN работает с провайдерами интернет-услуг и с операторами регистратур, чтобы убедиться, что у них есть все знания, все инструменты и вся необходимая поддержка для предоставления DNSSEC на следующих уровнях.

СИРАНУШ ВАРДАНЯН: Спасибо.

Сетонджи, у вас поднята рука?

Бетти, спасибо за помощь.

Затем слово получат Оливер и Фируз.

СЕТОНДЖИ ХУНЗАНДЖИ (SETONDJI HOUNZANDJI): Я буду говорить на французском. Спасибо. Меня зовут Сетонджи. Я системный администратор, и я управляю сервером Linux. Я родом из Бенина, но живу во Франции.

Мой вопрос касается ccTLD. Меня очень интересует все, что связано с DNS, и я работаю над тем, как обеспечить безопасность DNS-серверов. Мой вопрос относится к ccTLD, потому что, как вы знаете, во многих странах ccTLD и регистратуры назначаются решением правительства. И мы заметили, что очень часто ccTLD плохо настроены, плохо управляются, плохо администрируются. Моя проблема заключается в том, чтобы выяснить, возможно ли предложить ICANN провести аудит всех ccTLD, чтобы выпустить правила в отношении того, что должно быть сделано. Вы знаете, что на сегодняшний день многие ccTLD не внедрили DNSSEC. Что же делает ICANN?

Я бы хотел, чтобы ICANN заставляла людей. Так, например, вы можете начать аудит некоторых ccTLD и сказать им: «Вы не отвечаете современным требованиям, и мы не можем продолжать

вести с вами дела. Мы направим аудитора. Мы будем принуждать делать определенные вещи, чтобы вы могли обновляться», потому что, если европейские и американские ccTLD защищены, но не защищены африканские, то это проблема. Мы говорили, что ICANN — это один мир, один интернет, поэтому у нас не должно быть одного мира и многих интернетов.

Это был мой вопрос. Спасибо.

ДЖОН КРЕЙН: Хорошо, я разбил это на две части. Первая — некоторые заявления о состоянии среды ccTLD и их техническом статусе. И вы сделали несколько интересных замечаний, но я бы с удовольствием обсудил это отдельно, потому что я хотел бы увидеть, какие данные у вас есть, потому что, как исследователи и ученые, мы действительно заинтересованы в данных. Итак, вы сделали много заявлений о качестве инфраструктуры, и если у вас есть данные, подтверждающие это, мы бы хотели их получить. Если нет, то мы хотели бы провести дискуссию о том, что видно и что не видно. В частности, вы сказали, что многие ccTLD не подписаны. Я думаю, что это ваше мнение, потому что многие подписаны. Чтобы мы могли обсудить это на основе данных.

Другой аспект связан не с техническими вопросами, а с политикой управления ccTLD. Политика в отношении cTLD не устанавливается ICANN или внутри ICANN, но ccTLD — это коды стран, и у них другой механизм. Таким образом, у ICANN нет механизма, позволяющего проводить определенную политику в

этой области. Ее не существует. Что мы делаем, так это сотрудничаем с ccTLD, и это сотрудничество очень широкое. И Дэвид может рассказать о том объеме работ, которые мы ведем с ccTLD.

Поэтому именно такие форумы, как ICANN, являются местом, куда вы можете прийти и обсудить подобные проблемы и вопросы политики. ccNSO — это место, где многие ccTLD собираются вместе и работают над всеми этими вопросами. На большинстве конференций ICANN, если не на всех, проводится Tech Day, где обсуждаются эти вопросы.

Поэтому сейчас идет активное сотрудничество между ccTLD и ICANN, и особенно с некоторыми из моих сотрудников, по улучшению ситуации, но я думаю, что для аудита необходимо, чтобы мы были владельцами этого процесса разработки политики. И этот политический процесс происходит не в ICANN.

Поэтому нет, в обозримом будущем не возникнет ситуации, когда ICANN сможет зайти в регистратуру ccTLD и провести аудит. И с учетом того, как разрабатывалась эта политика, можно утверждать, что этого не должно быть, потому что это не входит в нашу компетенцию. Это не наша роль.

Ким, у вас есть что добавить к этому, или...

КИМ ДЭЙВИС: Да. Я думаю, это было хорошее резюме. Думаю, стоит еще раз подчеркнуть (поскольку многим из вас это может быть незнакомо)

разницу между доменом общего пользования верхнего уровня (gTLD) и национальным доменом верхнего уровня. Что касается доменов общего пользования верхнего уровня, то большая часть политического процесса, который происходит на подобной конференции ICANN, связана с установлением правил и требований, необходимых для работы gTLD, и параметров, в рамках которых они работают. И значительная часть работы ICANN заключается в том, чтобы после принятия сообществом этих правил внедрить их, а затем контролировать их соблюдение. Для этого в ICANN есть по контролю исполнения договорных обязательств. Каждый оператор gTLD должен соответствовать определенным требованиям, чтобы успешно продолжать его эксплуатацию. И если они не соответствуют этому показателю в течение длительного периода времени, то для этого существуют средства правовой защиты.

Похоже, что вы ищете какое-то подобное соглашение, возможно, для ccTLD, но для ccTLD это совсем другие отношения. Еще в самом начале существования DNS, в 1980-х годах, было принято решение — решение, которое сохраняется до сих пор — о том, что ccTLD действительно принадлежат соответствующим странам. Роль ICANN относительно ограничена: найти доверительного управляющего в стране, который будет управлять ccTLD для общественного блага. И концепция заключается в том, что в этой стране будут созданы все соответствующие механизмы надзора для обеспечения того, чтобы этот оператор оставался подотчетным и делал все необходимое. Очевидно, что это

сложный мир, в разных странах есть много разных механизмов для этого. Некоторые из них лучше, другие хуже. Это понятно.

Что ICANN может сделать положительного в рамках нашей деятельности по техническому взаимодействию и тому подобное, — это продвижение передового опыта для наращивания потенциала, помощь в информировании менеджеров ccTLD о том, каковы их обязательства и как выполнять эти обязательства. Управление ccTLD на национальном уровне — это очень мощный и фундаментальный компонент, операторы не имеют полного контроля, но в значительной степени отвечают на местном уровне за то, как они работают. Это означает, что наша миссия и наш мандат относительно ограничены, когда речь идет о ccTLD. Спасибо.

СИРАНУШ ВАРДАНЯН: Спасибо.

У нас какие-то [неполадки]?

Хорошо. Мы зададим еще один вопрос отсюда, затем один удаленный, а затем предоставим возможность Киму выступить с презентацией. И мы продолжим [игру с конфетами].

ОЛИВЕР РИСТЕСКИ (OLIVER RISTESKI): Здравствуйте, меня зовут Оливер. Я из Македонии. Я работаю в Министерстве внутренних дел. Кроме того, я являюсь сотрудником Центра исследований в области

безопасности. Мой вопрос связан с тем, что недавно мы столкнулись с получением электронных писем с фальшивыми сообщениями о минировании в государственных школах, аэропортах, торговых центрах и транспортных центрах. Это потребовало от нашего министерства больших ресурсов. Отслеживание этого вида преступлений крайне низкое. И эффективность раскрытия/расследования этого вида преступлений крайне низка. Кроме того, этот вопрос является общим для всех [неразборчиво] Балкан. Есть ли возможности для проведения исследований по этим вопросам?

ДЖОН КРЕЙН: Похоже, что вы говорите в основном о фишинговых эксплойтах и т. д., вредоносных программах и тому подобных вещах, которые просто отвратительны и являются частью нашей повседневной жизни в Интернете. Да, мы можем проводить исследования в этой области, когда речь идет о системе доменных имен.

И я не знаю, Саманех, не хотите ли вы немного рассказать о некоторых исследованиях, которые мы проводим.

САМАНЕХ ТАДЖАЛИ (SAMANEH TAJALI): Спасибо за ваш вопрос, Оливер, и спасибо, Джон. Как упомянул Джон, это повседневная типичная проблема, с которой сталкивается большинство пользователей Интернета. В настоящее время мы в группе SSR проводим исследования по этому вопросу. Скоро будет опубликовано:

выявление методов или более эффективных методов классификации фишинговых писем в различные категории спама, вредоносного ПО и т. д. Так что продолжайте знакомиться с нашими документами или публикациями OCTO. Мы планируем опубликовать наши методы. Сначала мы собираемся опубликовать научную работу, а после того, как она пройдет рецензирование, мы опубликуем методику. Возможно, эти методы полезно внедрить в других областях, у провайдеров, операторов и т. д.

ДЖОН КРЕЙН: Есть и другие вещи, о которых можно подумать. Если у вас есть национальная группа CERT, убедитесь, что она является членом FIRST, который является органом CERT во всем мире. Сама ICANN фактически является членом FIRST, который представляет собой форум для групп быстрого реагирования. Так что участвуйте в жизни этого сообщества. Убедитесь, что ваши специалисты по реагированию на инциденты входят в сообщество специалистов по реагированию на инциденты, потому что эта проблема не является уникальной для кого-либо.

Другое, что вы можете сделать в долгосрочной перспективе, — это инвестировать в свои университеты, в развитие талантов и страны, чтобы понимать все это, будь то исследования или реагирование на инциденты, или даже просто хорошие навыки работы в сети и т. д., как в технических сетях. Это еще одно, что вы можете сделать.

Если вас действительно интересуют в основном аспекты общественной безопасности, связанные с использованием Интернета, и вы задаетесь вопросом, как вы можете повлиять на политику в этой области или принять участие в ее разработке, у нас есть Правительственный консультативный комитет. Это очень важная часть процесса ICANN. И в этом комитете есть рабочая группа по обеспечению общественной безопасности. Так что если ваше правительство участвует в GAC, и у них есть особый интерес к этой области, то Рабочая группа по обеспечению общественной безопасности — это то, на что им стоит обратить внимание и принять участие в ее работе.

Сейчас в ICANN мы занимаемся тем, что называем техническими злоупотреблениями или угрозами безопасности, связанными с системой идентификаторов. Не все угрозы, которые вы видите в Интернете — на самом деле, многие угрозы, которые вы видите в Интернете — не связаны с вашей работой. Но эта конкретная тема всегда остается актуальной в ICANN. И в данный момент в сообществе происходят различные события. Ведутся переговоры по контрактам на тему того, что значит быть регистратурой и регистратором и что нужно делать в отношении злоупотреблений DNS. В действующем контракте говорится, что вы должны получать сообщения и расследовать их. Это не точный текст контракта, но я не юрист. Но одна из вещей, отсутствующих в формулировках контрактов, заключается в том, что эти люди должны смягчать последствия злоупотреблений. И мы работаем по запросам сторон, связанных договорными обязательствами —

регистраторов и регистратур. Они пришли к нам и сказали: «Мы хотим добавить это в наш контракт, чтобы по договору мы были обязаны смягчать последствия злоупотреблений». Эта дискуссия продолжается в настоящее время.

Мы проводим много тренингов. Саманех и наша группа проводят множество исследований и делают много публикаций в этой области. Так что это нас очень, очень интересует.

Если у вас есть правоохранительные органы, которые хотели бы поговорить с нами о просвещении и информировании, мы будем рады пообщаться с ними. В нашем штате есть люди, которые проводят много времени, общаясь с представителями правоохранительных органов по всему миру. Наша основная задача — объяснить им, как работает экосистема, а иногда и знакомить их с другими участниками экосистемы, создать доверие, если хотите, потому что это очень важно для нашей способности выполнять работу для всех.

Так что приходите к нам, и мы сможем обсудить с вами в личной беседе, как мы можем помочь вашему министерству и правительству принять более активное участие.

СИРАНУШ ВАРДАНЯН: Спасибо.

Могу я попросить техническую команду организовать презентацию IANA?

Тем временем я буду озвучивать вопросы удаленных участников. Ромуло Чачин, участник Программы NextGen на ICANN76, хотел бы узнать, как различные проекты и программы по снижению угроз безопасности взаимодействуют между собой.

ДЖОН КРЕЙН: Сколько у вас времени? Я имею в виду, что если вы посмотрите на основные полномочия ICANN, если вы посмотрите на наш устав, если вы посмотрите на цель ICANN, то там очень четко сказано, что мы должны беспокоиться о безопасности, стабильности и устойчивости Интернета, систем идентификации. То есть это не сайты отдельных людей и т. д., но это имя, которое... Здравствуйте. Здравствуйте, соседи. Я слышу... Хм, я слышу голоса.

Так что в некотором смысле это основа всего, что мы делаем. Все взаимодействует с безопасностью. Каждый раз в ICANN в качестве сотрудников, а также в большинстве случаев в качестве сообщества, когда мы что-то рассматриваем, мы всегда помним об этом. Как это влияет на безопасность? Как это влияет на стабильность? Так что все взаимодействует.

В рамках нашей группы — а я познакомил вас с кучей людей в IROS — IANA хорошо выполняет свою работу, что они всегда делают, потому что они потрясающие, это критически важно для безопасности системы и стабильности системы. Нам нужна хорошая регистрация идентификаторов. Затем мы проводим исследования, занимаемся информированием и образовательной деятельностью. Вот чем мы занимаемся. Но мы также, как сказал

Ким, занимаемся вопросами соблюдения наших контрактов. Мы ведем переговоры по контрактам. У нас есть возможность участвовать во всех этих обсуждениях политики. И все влияет на безопасность и стабильность систем идентификации, потому что, когда доходит до дела, это наша работа. Вот чем мы занимаемся.

СИРАНУШ ВАРДАНЯН: Спасибо.

Ким, вам слово для представления работы IANA, пожалуйста.

КИМ ДЭЙВИС: Разумеется. Нам показалось хорошей возможностью, пока мы ведем это обсуждение, провести краткий экскурс по функциям IANA. Это то, что вы, вероятно, часто услышите во время конференции ICANN. А термином «IANA» бросаются тут и там, предполагая, что вы знаете, что он означает. Таким образом, это лишь относительно краткий обзор того, из чего состоят функции IANA. И, надеюсь, это тоже будет познавательно. После этого мы продолжим отвечать на вопросы. Так что если появится что-то, на чем вы хотели бы остановиться подробнее, пожалуйста, дайте нам знать.

Мы уже немного говорили об этом: IANA, Администрация адресного пространства Интернет. Несмотря на название, мы занимаемся не только нумерацией. Мы занимаемся и именами. Мы разрабатываем параметры протоколов. Мы занимаемся всевозможными идентификаторами.

По сути, это один из старейших институтов Интернета. В самые первые годы существования Интернета, когда это был исследовательский проект, когда в конце 1960-х и начале 1970-х годов были подключены первые узлы, кому-то нужно было вести учет того, какие компьютеры к кому подключены. И эту роль в самом начале играл человек по имени Джон Постел. Это человек справа на экране рядом с Винтом Серфом. И Джон Постел в самом начале был воплощением IANA.

Позже IANA получила свое название и стала чем-то вроде имени, которым разбрасывались в 1980-х годах. IANA стала больше, чем просто один человек. Она стала командой.

Но, в конечном счете, такова была его первоначальная цель в те времена, и такова она остается и сегодня: для чего используются идентификаторы, и где есть аутентичная запись того, для чего эти идентификаторы были сделаны?

Поэтому именно в 1990-х годах было признано, что функции IANA в частности и управление корневой зоной действительно нуждаются в более формальной структуре, чем просто один ученый (Джон Постел работал в университете) мог сделать лично и со своей командой. На протяжении 90-х годов предпринимались попытки формализовать это, чтобы признать коммерциализацию Интернета, рост Интернета и растущие требования к функции IANA.

ICANN была создана для того, чтобы стать домом для IANA. Такова была ее первоначальная компетенция. На самом деле, до того, как

у ICANN получила свое название, она называлась «Новая IANA». И сегодня ICANN по-прежнему существует для этой фундаментальной цели. У ICANN есть и другие полномочия в области идентификации, помимо IANA, но IANA по-прежнему является основой миссии ICANN.

И сегодня IANA — это департамент ICANN, который ведет реестры (и я использую здесь слово «реестры» в общем смысле — не регистратуры доменов, а реестры в смысле официальной записи) уникальных идентификаторов Интернета. Каждый из этих реестров имеет свою политику, поэтому часть работы нашей команды заключается в применении этих политик в зависимости от типа идентификатора и ситуации. Поэтому, когда вы слышите «IANA», это означает функцию распределения, функцию официального хранителя записей, которой занимается отдел IANA в ICANN.

Так зачем же нужен официальный регистратор, такой как IANA, для Интернета? Разве Интернет не свободен от какого-либо централизованного контроля? Компьютеры общаются друг с другом с помощью технических протоколов, и очень важно, чтобы эти технические протоколы были одинаковыми, чтобы компьютеры понимали друг друга. В то время как содержимое передается по этим протоколам, основными протоколами являются, например, TCP/IP.

Они должны работать одинаково на каждом устройстве, чтобы сеть просто функционировала, поэтому большая часть работы,

которую мы проводим в IANA, касается не столько протоколов, которые вы видите, например, доменных имен, сколько вещей, которые работают на более низких уровнях вашего компьютера и сетевого устройства, чтобы гарантировать, что передача между различными устройствами Интернета работает, является точной, что отправленный файл-вложение будет получен на другом конце в правильном формате, и что при подключении к сервису вы не получите голосовой вызов вместо веб-сайта. Речь идет о вещах такого рода. Таким образом, все эти идентификаторы имеют определенное назначение, чтобы помочь этому общению. И они используются в основном поставщиками программного обеспечения. Поставщики программного обеспечения используют эти назначения IANA, чтобы убедиться, что их программное обеспечение работает со всеми остальными в Интернете.

Поэтому сегодня эти функции выполняет команда IANA. Существует несколько различных контрактов. Честно говоря, это довольно сложная путаница контрактов, но, тем не менее, существует довольно много контрактов, которые определяют, как сегодня выполняются функции IANA.

Еще один термин, который вы, возможно, знаете или слышали на этой неделе — PTI. PTI – аффилированная организация ICANN. Считайте, что это дочерняя компания ICANN, которая фактически выполняет функции IANA. Для большинства намерений и целей PTI не является заметным органом. Одна из гарантий, которые были реализованы в 2016 году, когда произошла передача полномочий

на основе модели с участием многих заинтересованных сторон ICANN, заключалась в передаче функций IANA в организацию, отличную от ICANN, но контролируемую ICANN, и это PTI. Вы еще услышите о PTI. Мой совет: не стоит слишком сильно переживать из-за термина PTI. Просто знайте, что это официальное юридическое название организации, которая выполняет функции IANA.

Повседневная деятельность? Мы функционируем так же, как и любой другой отдел ICANN. Нас около 16 человек, и это наш хлеб с маслом. В этом заключается наша работа.

Итак, каковы функции IANA, только немного подробнее? Обычно мы делим их на три раздела: параметры протокола, ресурсы нумерации и доменные имена. Это различие несколько условно. Эти сегменты немного пересекаются. Но для общего обсуждения функций IANA вполне подходит разделение на эти три области.

Первое, на чем я остановлюсь, — это параметры протокола, потому что они, по сути, являются самым фундаментальным аспектом того, что мы делаем. Параметры протокола. Существуют тысячи различных типов параметров протокола. Существуют сотни тысяч, если не более миллиона, назначений параметров протокола. Они многочисленны. Их множество. О 99% из них никто из вас даже не слышал. О 98% из них я даже не слышал. Их много. И многие из них используются в очень специфических приложениях. Если вы не создаете программное обеспечение для выполнения очень специфических задач, возможно, вам никогда не

понадобится использовать один из этих реестров. Но для пяти, десяти или 50 человек, которые работают в очень специфической отрасли, внедряющей программное обеспечение в сфере одного из этих наборов уникальных идентификаторов, работа, которую выполняет IANA, бесценна. На сайте IANA.org/protocols есть указатель, если вы хотите получить представление о полном списке, но их там очень много.

В отношении параметров протокола IANA играет непосредственную роль в том, что реализаторы, которые часто являются поставщиками программного обеспечения и разработчиками протоколов, обращаются непосредственно в IANA, разговаривают с нашей командой и получают необходимые им распределения непосредственно от нас. Это ключевое отличие от доменных имен и ресурсов нумерации, о котором я расскажу чуть позже, потому что, вообще говоря, люди приходят в IANA не для того, чтобы получить доменное имя. Люди приходят в IANA не для того, чтобы получить ресурсы нумерации. Вместо этого у них есть иерархические системы распределения, где есть посредники. Есть разные люди с разными обязанностями. IANA играет лишь небольшую роль в истории распределения. И отчасти это связано с тем, что существует гораздо больше правил для применения ресурсов нумерации и доменных имен.

Откуда появляются эти реестры параметров протокола? Подавляющее большинство из них разрабатывается в IETF (Инженерная проектная группа Интернета). Это основной орган по стандартизации Интернета. Именно здесь происходит большая

часть стандартизации Интернета — не вся, но большая часть. И когда люди разрабатывают стандарты Интернета в IETF, одним из компонентов этого является разработка реестров IANA для этих стандартов Интернета.

Возможно, вы слышали об RFC. Это серия документов, в которой публикуются стандарты Интернета. И многие RFC либо создают, либо ссылаются, либо изменяют реестры IANA. Они включают инструкции о том, что должна делать IANA и какие правила она должна соблюдать.

Немного поговорим о ресурсах нумерации. Для тех, кто не знаком: ресурсы нумерации обычно относятся к трем ключевым вещам: Адреса интернет-протокола 4-й версии, адреса интернет-протокола 6-й версии и номера AS. Для тех, кто не знаком с IP-адресами, есть две разновидности: v4 и v6. Это уникальные номера, которые присваиваются каждому устройству в Интернете. Он есть у вашего ноутбука. Он есть у вашего телефона. Он есть у вашего умного устройства в доме. Возможно, он есть у вашего телевизора. Они появляются у все большего количества различных вещей в мире, и это уникальный идентификатор, который используется для передачи от одного устройства к другому. По своей сути, когда передача осуществляется через Интернет, каждая передача, известная как пакет, должна иметь адрес «От кого» и адрес «Кому». «От кого» и «Кому» — это IP-адреса.

Поскольку этих адресов буквально миллиарды, вам нужен какой-то способ объединить их в большие наборы, чтобы это было легко

сделать, чтобы сетевым инженерам не приходилось вводить каждый IP-адрес по отдельности. Для этого используются номера автономных систем, или номера AS. Мне нравится думать о номерах AS так: это что-то вроде почтовых индексов Интернета. Сетевые провайдеры группируют большие наборы IP-адресов под одним номером — номером AS — и затем, когда они говорят о том, куда направлять трафик через Интернет, они используют номера AS, чтобы облегчить эту задачу.

Итак, я рассказал о том, что это такое. Отмечу, что IP-адреса версии 4 у нас все закончились. Мы раздали последние доступные адреса IPv4 несколько лет назад. Региональные интернет-регистратуры, которые присваивают их сетям, также в основном не работают. Таким образом, предложение IPv4 очень ограничено, поэтому вы можете услышать, что существует много инициатив по переходу на версию IPv6, где гораздо больше возможностей для роста Интернета.

Я только что упомянул о региональных интернет-регистратурх. Для тех, кто не знаком с этой концепцией, я уже упоминал, что вы не обращаетесь напрямую в IANA за IP-адресом. Происходит это так: вам как конечному пользователю автоматически присваивается IP-адрес вашим сетевым провайдером. Они используют протокол DHCP — еще один из тех протоколов, над которыми работает IANA. DHCP выделяет вам IP-адрес индивидуально для каждого устройства. Каждый сетевой провайдер, будь то ваш интернет-провайдер или конференц-сеть

отеля, имеет набор IP-адресов, которые они делят между людьми в своем учреждении или в своей сети.

Где они берут свои блоки? Они обращаются в региональную интернет-регистратуру. Существует пять региональных интернет-регистратур. LACNIC — это региональная интернет-регистратура Мексики. И для каждого из них хлебом насущным является присвоение этих номеров AS и IP-адресов сетевым операторам в их регионе. RIR, в свою очередь, получают распределения от IANA.

Наконец, доменные имена. Какова роль доменных имен? Я это пропущу. Итак, в иерархии DNS наиболее важной частью пространства доменных имен является корневая зона. И это важная часть того, что мы делаем в IANA. Чуть ниже корня на этой схеме можно увидеть домены верхнего уровня. В свою очередь, они присваивают метки до этого, домены второго уровня, и так далее, и так далее.

Итак, нашей основной обязанностью в рамках IANA является администрирование корневой зоны DNS — опять же, это аутентичная запись о том, что такое домен верхнего уровня, а также вся техническая информация, которая связана с этим, а также административная информация, например, кто является контактными лицами? Какая компания на самом деле управляет этим TLD? Речь идет о вещах такого рода. И мы являемся официальным регистратором этих фактов. Мы получаем от этих операторов запросы на внесение обновлений и административных изменений в их TLD. Мы проводим тщательную

проверку по определенным типам запросов. А затем, когда IANA убедится, что любые изменения в корне DNS являются целесообразными, мы направляем их для внедрения в корневые серверы DNS.

Я уже упоминал об этом ранее в ответ на вопросы, так что я буду краток, но мы управляем ключом для подписания ключей, центральным ключом, который также защищает DNS. Мы делаем это на церемониях подписания ключей. Причина, по которой мы делаем это очень публично, заключается в укреплении доверия. Мы могли бы сделать всю нашу работу по DNSSEC и обеспечению безопасности Интернета в частном порядке и просто сказать: «Эй, мы — ICANN. Доверьтесь нам», но лучший способ сделать это — вовлечь всех вас в процесс, дать сообществу доступ, видимость. И мы считаем, что это способствует повышению доверия, потому что каждый может увидеть все своими глазами. Они могут посмотреть на то, что они делают, а эксперты по безопасности со всего мира могут посмотреть на то, что мы делаем, и все вместе посмотреть на это и сказать: «Да, это делается безопасным и надежным способом. Мы можем доверять этой системе».

Некоторые другие функции мы выполняем и в доменных именах. Мы управляем доменом .int, одним из доменов верхнего уровня. Он предназначен исключительно для межправительственных организаций. Он недоступен для общей регистрации. Мы также управляем доменом .arpa. Я бы вкратце описал .arpa как техническую сантехнику. Это домен, который вы, скорее всего, никогда не увидите напрямую, но он важен для определенных

операций в Интернете. Кроме того, у нас есть хранилище наборов правил генерации меток. Именно здесь регистратуры, управляющие интернационализированными доменными именами, обмениваются передовым опытом и придерживаются его.

Таков объем операций IANA. Очевидно, что это очень общее описание. Но в заключение я хотел бы отметить безопасность. Вообще-то, знаете что? Я пропущу этот слайд. Некоторые другие аспекты IANA.

Я думаю, что в основе всего, что мы делаем, лежат беспристрастность и нейтральность. Мы здесь для того, чтобы проводить политику в том виде, в котором она написана. Мы можем давать рекомендации, но в нейтральном ключе. Это часть того, чем мы занимаемся на этой неделе. Мы уделяем большое внимание эффективности. Существует множество SLA, которые регулируют нашу работу. Мы постоянно измеряем то, что мы делаем. Мы постоянно отчитываемся о проделанной работе. Это ключевой момент. Мы хотим постоянно совершенствоваться, поэтому это еще одна часть нашей работы — постоянное улучшение. Частью этого является проведение внешних аудитов третьей стороной и общая подотчетность сообщества. Существует множество комитетов по надзору и т. п. за IANA, о которых вы узнаете в пространстве ICANN.

Итак, вкратце, IANA ведет реестры уникальных систем нумерации. Они нужны для обеспечения взаимодействия Интернета.

Большинство реестров IANA довольно просты. Люди обращаются непосредственно в IANA. Возможно, вы никогда не слышали о них. Они довольно просты, но есть и сложные, масштабные. Мы говорили о корневой зоне. Мы говорили о ключе, который защищает корневую зону. И для них IANA является своего рода глобальным корнем для этих систем именования.

Таков взгляд на IANA с высоты 10 000 метров. Спасибо.

СИРАНУШ ВАРДАНЯН: Спасибо, Ким. Это было очень информативно. А для наших участников эта презентация PowerPoint загружена на сайт ICANN76 под подробным описанием этой конкретной сессии. Так что если вы хотите скачать ее и использовать, смело делайте это.

И теперь мы можем задать еще несколько вопросов. На это у нас отведено 30 минут. Поэтому не стесняйтесь

Фируз, да, я знаю, что вы в очереди. Прошу вас, Фируз. Я вижу Дэвида? Да. Но мы начнем…

ФИРУЗ АЗИМОВ: Здравствуйте! Меня зовут Феруз. Я участник программы Fellowship ICANN. Я ждал, и у меня уже есть два вопроса. Мой первый вопрос о... Как мы уже упоминали ранее о проблеме Meta, я помню, что также была другая проблема с Meta: в том, что подсеть Meta была заявлена другим провайдером. И такое обычно случается. В нашей стране мы столкнулись с такой проблемой: наша подсеть,

выделенная для DNS, была заявлена другим провайдером. И мы потеряли Интернет не только для этой подсети, но и для всех наших пользователей. И мой вопрос в том, есть ли [неразборчиво] решение для предотвращения такого рода проблем. И каждый пограничный маршрутизатор в Интернете должен иметь включенную проверку RPKI перед установкой [маршрута] в таблице маршрутизации. И как мы можем предотвратить это и обеспечить стабильность, как вы упомянули, в нижних слоях (например, в слое 3)?

ДЖОН КРЕЙН: Итак, это еще одна дискуссия о том, как мы обеспечиваем безопасность маршрутизации. То, о чем вы говорите, часто называют захватом BGP.

Я передаю слово Дэвиду, чтобы он немного рассказал об этом.

ДЭВИД ХУБЕРМАН: RPKI в некоторой степени помогает решить эту проблему. Интересно то, что проблема, которую вы только что описали, происходит каждый день в Интернете, иногда несколько раз в день. Наши друзья из Общества Интернета фактически создали обсерваторию для наблюдения за этими событиями, и они регистрируют 500-1000 таких событий каждый год. И это продолжается с 1990-х годов. Ничего нового. Некоторые из них являются злонамеренными. Некоторые из них предназначены для тех, кто по каким-то причинам хочет пошалить. Во многом это

случайность, потому что в течение многих, многих лет инженеры, создающие Интернет, вводили конфигурации в маршрутизаторы вручную. Мы люди, и мы делаем опечатки. Мы делаем ошибки. И когда вы допускаете ошибку в маршрутизаторе, это может привести к очень плохим последствиям. RPKI призван помочь в решении многих из этих проблем, но особенно во втором сценарии, особенно в случае неправильной конфигурации, допущенной человеком. RPKI очень помогает.

Что мне нравится в RPKI, так это то, что она не требует, чтобы каждый маршрутизатор, использующий BGP, проверял объявления. На самом деле для этого требуются только для самых крупных транзитных сетей в мире, потому что, когда мы передаем информацию о маршрутизации от вашего министерства, от вашего интернет-провайдера, к сети конференции ICANN здесь, в Канкуне, к Facebook в Калифорнии, к чему-то в Венесуэле или еще где-то, все эти пакеты обычно проходят через довольно небольшое число — около 800 или около того — крупных интернет-провайдеров, которые обеспечивают транзит этих пакетов. И оказалось, что если только эти 800 или около того провайдеров проверяют и подписывают маршруты, то все недействительное отбрасывается, и трафик не попадает туда, куда не должен попадать.

Так что одной из историй успеха RPKI и безопасной маршрутизации в целом за последние несколько лет является 100% принятие 800 или около того крупнейших интернет-провайдеров в мире для проверки пакетов, что означает, что если

вы управляете сетью или регулируете ряд сетей, то критически важно, чтобы эти сети выдавали сертификаты, ROA (подтверждения источника маршрута) для своих префиксов маршрутизации, чтобы все могли проверить их.

Для полной защиты канала, для полной защиты коммуникаций нам нужен не только RPKI. Нам также необходимо подтвердить путь. Пакет, когда он покидает ваше устройство и направляется к месту назначения, а затем возвращается обратно, проходит через ряд промежуточных сетей, и нам необходимо обеспечить проверку этого пути на протяжении всего времени, чтобы кто-то не мог взять этот пакет и начать его обрабатывать, когда мы не уполномочили его на это. Это называется «атака посредника».

IETF, инженерное сообщество, имеет некоторые решения. Мы продолжаем работать над лучшими решениями, которые смогут внедрить все. И это будет следующим этапом нашего пути в мире безопасности маршрутизации.

СИРАНУШ ВАРДАНЯН: Спасибо.

Дэвид, если мы можем перейти к... А потом Николас. Я знаю, что у вас есть вопрос об IANA.

ДЭВИД ИОНДРАГОН (DAVID MONDRAGON): Приветствую всех. Это Дэниел из NIC Costa Rica, старший сетевой инженер. NIC Costa Rica отвечает за

домены TLD в Коста-Рике. У меня два вопроса. Первый вопрос: предпринимает ли ICANN или IANA какие-либо усилия, чтобы внедрить политики или технологии использования DNS или TLS вместо DNS по HTTPS? Потому что это может быть проблемой для большинства сетевых инженеров.

Второй вопрос — какова точка зрения IANA и ICANN на этот вопрос в плане политики маршрутизации и безопасности?

ДЖОН КРЕЙН: Первый вопрос простой. Ответ — нет, потому что это не входит в наши полномочия. Мы изучаем эти вещи. Мы их измеряем. Мы ими интересуемся. В других областях ведется много дискуссий о влиянии этого. Если вы проводите исследование, смотрите на пакеты DNS и хотите заглянуть в них, очевидно, вы не сможете сделать это в рамках [DAAR] и тому подобного. И вы можете поспорить. Это хорошо? Это плохо? Я не знаю ответа, поэтому я просто говорю с личной точки зрения, потому что в таких технологиях всегда есть противоречие между безопасностью и конфиденциальностью.

Поэтому я не думаю, что у нас есть какая-то особенная официальная позиция в отношении DoH. Мы провели некоторые исследования по этому вопросу.

И поскольку Мэтт был очень тихим, я хочу посмотреть, не уснул ли он еще, и хочет ли он поговорить об этом.

МЭТТ ЛАРСОН (MATT LARSON): Да. Я здесь не сплю. Да, мы провели некоторые исследования DNS по HTTP и DNS по TLS. На самом деле, Пол Хоффман из исследовательской группы внес свой вклад в эти усилия с точки зрения стандартов. На самом деле мы помогли разработать эти стандарты.

Учитывая общий растущий интерес к конфиденциальности, я думаю, что мы неизбежно увидим, что эти протоколы развертываются все больше и больше.

В то же время, однако, они требуют больших вычислительных затрат и более требовательны к сети, поскольку обычный DNS — это просто один пакет для запроса и один пакет для ответа. И, возможно, это происходит через TCP-соединение, в этом случае происходит обмен несколькими пакетами для установления и разрыва этого соединения.

Но как только вы начинаете говорить о добавлении к этому криптографии, вы говорите о все более сложных взаимодействиях с большим количеством пакетов. И провайдеры, которые отвечают на большое количество DNS-запросов, такие как операторы TLD и операторы корневых серверов, немного нервничают по поводу того, что это означает для их инфраструктуры. Если вдруг каждый поступающий запрос будет представлять собой не просто один пакет по UDP, а потребует установки соединения и криптографической проверки, это требует гораздо больших затрат. И поэтому у людей, управляющих

критически важной инфраструктурой в больших масштабах, возникают опасения и вопросы по этому поводу.

Но я думаю, что как отрасль и как общество мы движемся именно в этом направлении. Поэтому я думаю, что мы неизбежно увидим более активное развертывание этих протоколов.

СИРАНУШ ВАРДАНЯН: Спасибо.

Извините, Дэниэл. Я назвала вас Дэвидом.

Николас? Мы ответим на еще один вопрос Николаса, а затем Дэвид представит всем нам программу KINDNS. Спасибо.

НИКОЛАС ФУМАРЕЛЛИ: Спасибо. Я виртуально участвовал в последнем обновлении ключа KSK на прошлой неделе, кажется. Это вопрос, связанный с этим, а также с [неразборчиво] DNSSEC. Ведутся ли в IETF какие-либо работы по включению постквантовой криптографии в протокол DNSSEC, особенно в отношении администрирования корневой зоны? Учитывая, что в IETF уже предпринимаются усилия по включению постквантовых алгоритмов в другие протоколы, какие проблемы ожидает команда PTI при внедрении этих новых алгоритмов в DNSSEC, и как вы планируете решать эти проблемы для обеспечения безопасности и стабильности системы DNS? Спасибо.

КИМ ДЭЙВИС: Благодарю за вопрос. На данный момент у нас нет никаких инициатив в области пост-квантовой криптографии, но мы проводим подготовительную работу по изменению криптографического алгоритма в корневой зоне. Сегодня мы используем RSA-SHA256. И мы никогда не меняли этот алгоритм. И неясно, будет ли изменение алгоритма трудным или легким. В последние несколько недель мы создали в сообществе группу разработчиков. Они встретятся через две недели в Иокогаме, чтобы подробно обсудить этот вопрос. Цель группы разработчиков — определить, как изменить алгоритм в корневой зоне, будь то пост-квантовая криптография или, возможно, что-то другое, например, алгоритм криптографии с эллиптической кривой, чтобы уменьшить размер пакетов [и] получить другие положительные результаты.

Сейчас мы на этом этапе.. Я думаю, что преждевременно начинать думать о пост-квантовой криптографии. Это определенно, я бы сказал, отдаленная перспектива.

Но если говорить о том, что происходит в этом пространстве, я, пожалуй, передам слово Мэтту, чтобы он рассказал об исследовательской деятельности, потому что с моей операционной точки зрения, я думаю, что постквантовая криптография в настоящее время больше исследовательская деятельность.

МЭТТ ЛАРСОН (MATT LARSON): Спасибо, Ким. Благодарю за вопрос. Для меня это возможность обратиться к серии документов OCTO, о которой Джон упоминал несколько лет назад. Мы написали документ об этом. Я не нахожусь в комнате Zoom, поэтому не могу вставить ссылку, но он называется OCTO-031: Квантовые вычисления и DNS. И это как раз на эту тему. Поскольку пост-квантовые криптовалюты привлекают все больше внимания, OCTO поручила одному криптографическому исследователю, очень известному, провести исследование пост-квантовых криптовалют и написать об этом статью. Так что она читабельна, но это напряженная работа. Поэтому мы сделали более общую версию, и это OCTO-031. И это наше мнение о состоянии индустрии и о том, чего нам стоит опасаться в пост-квантовой криптографии. И я думаю, что ответ таков: мы еще очень, очень далеки от того, чтобы беспокоиться о постквантовых алгоритмах, потому что мы еще очень, очень далеки от квантового компьютера, который даже отдаленно сможет представлять угрозу для алгоритмов, которые мы сегодня используем для криптографии с открытым ключом.

Я думаю, это пример того, что в отрасли много шумихи, и люди говорят об этом. И ощущение, которое у вас может возникнуть при чтении отраслевых изданий, таково: «О, Боже! Это неизбежно, мир рушится, и мы все должны быть готовы!». И это не значит, что мы не должны быть готовы, но у нас есть годы, если не десятилетия. Так что, на самом деле, наша позиция такова: исследовать это еще слишком рано. У нас так много времени, потому что мы так далеки

от создания квантового компьютера, который мог бы стать угрозой для сегодняшней криптографии.

СИРАНУШ ВАРДАНЯН: Спасибо, Мэтт. Ссылка была размещена в чате в пространстве Zoom. Вы открываете его и читаете подробности в документе.

Тем временем, я хотела бы предоставить слово Дэвиду, чтобы он рассказал о проекте KINDNS.

ДЭВИД ХУБЕРМАН: Спасибо, Сирануш. Я хотел бы сменить тему на несколько оставшихся у нас минут и рассказать вам о том, что мы делаем в ICANN, чтобы попытаться помочь улучшить техническое состояние Интернета.

Вчера вечером я пошел ужинать. Я пошел в ресторан с другом и очень хорошо провел время. И пока нам подавали ужин, официант сделал то, что я считаю кошмарным сценарием для официанта. Наполняя мой стакан, он вылил на меня весь мой напиток и полностью промочил мою одежду. Когда такое происходит, я думаю, есть два или три способа, которыми мы можем реагировать как человеческие существа. Мы можем разозлиться и закричать: «Что?! Что вы делаете?!» и устроить сцену, и это просто трудно и неловко для всех. А можно сидеть и не реагировать. Или мы можем использовать наилучший подход: мы можем рассмеяться, улыбнуться и сказать: «Все в порядке. Вы совершили ошибку. Не

беспокойтесь, мой друг». Мы можем взять плохую ситуацию и сделать ее хорошей.

Ладно, мы сделали это вчера вечером, и официант был в порядке, мы посмеялись, мы друзья, и ничего страшного. Все нормально. К чему я это рассказываю? Потому что мы можем сделать то же самое в DNS. Мы можем быть добрыми, мы можем сделать жизнь лучше для всех, совершая определенные поступки, маленькие поступки, проявляя доброту друг к другу.

ICANN создала программу под названием KINDNS. Это веб-сайт — KINDNS.org. Цель этой инициативы для всех операторов DNS, больших и малых, будь то Google или Facebook, или новый небольшой интернет-провайдер в Македонии... Кем бы вы ни были, есть шаги, которые вы можете предпринять как оператор DNS, чтобы быть более добрым. И если все будут более добрыми, то и сама DNS сможет укрепить и улучшить свою техническую базу.

В этом проекте вы классифицируетесь как тип оператора, которым вы являетесь. Вы эксплуатируете небольшой частный рекурсивный резолвер. Вы управляете авторитативным сервером, который дает ответы на имена и вопросы DNS. Или, возможно, у вас публичный резолвер, и вы хотите, чтобы все в мире могли использовать его. В рамках проекта KINDNS вы можете провести самооценку как оператор и посмотреть, как у вас обстоят дела, оценивая их в сравнении с набором норм, которые сообщество — ICANN и техническое сообщество DNS — согласовали как базовый набор стандартов, которых должны придерживаться все, и если бы

все их придерживались, DNS работала бы лучше. Она была бы более надежной и стабильной. Вы можете провести тестирование по этому набору норм и посмотреть, как у вас идут дела, получить частный результат, чтобы увидеть, где вы находитесь, и, если есть пробелы, у вас есть возможность их устранить.

И эта работа проводится по образцу того, что, опять же, наши друзья из Общества Интернета сделали в области защиты маршрутизации. Они называли это хорошими манерами. Мы называем это добротой. Благодаря таким инициативам все сообщество может работать над улучшением ситуации для всех и делать это с помощью очень небольшого ряда шагов, которые, как правило, не стоят денег и не отнимают много времени. Это просто поможет вам понять, где находится ваша сеть, и внести небольшие изменения, чтобы улучшить эту сеть и инфраструктуру DNS, чтобы все могли извлечь выгоду.

Вот что такое KINDNS. Если у вас будет возможность, когда у вас появится свободное время, загляните на сайт KINDNS.org. И вы найдете там очень простые описания некоторых общепринятых норм, которых, по нашему мнению, должны придерживаться все.

И это все, чем я хотел поделиться с вами. Спасибо.

СИРАНУШ ВАРДАНЯН: Спасибо, Дэвид.

У нас удаленный вопрос от Мохамеда Эльнура Абдельхафеза Фадула из ISOC Судана. «Проверка пути важна для безопасности

глобальной таблицы маршрутизации. Для устранения этой проблемы было введено расширение BGPsec, но оно сталкивается с трудностями в развертывании из-за огромных ресурсов, потребляемых BGPsec. Необходимы исследования для оптимизации расширения и его развертывания. Какова роль ICANN в этом вопросе?».

ДЖОН КРЕЙН: Мы можем играть здесь две роли. Первая — это, конечно, взаимодействие, а второе — участие в исследованиях.

Так что я передаю слово, я думаю, Дэвиду. Ответите на этот вопрос?

ДЭВИД ХУБЕРМАН: Это отличный вопрос. Спасибо. Как я уже говорил ранее, два пути к безопасной инфраструктуре маршрутизации —- это RPKI и проверка пути. И, как справедливо отмечается в вопросе, у нас уже есть решение. IETF уже разработала решение под названием BGPsec — предположительно, безопасность BGP, верно? Но, как отмечает наш друг, развертывание BGPsec сейчас не очень реалистично, потому что вычислительные затраты маршрутизатора настолько огромны... Мы не сломаем Интернет. Нет, мы бы сделали что-то намного, намного хуже. Мы бы замедлили его.

Так что для ICANN наше участие в исследовании и участии в других решениях в некоторой степени заключается в том, что будет

делать команда Мэтта и другие команды в ICANN в плане участия в процессах разработки стандартов протоколов — я имею в виду IETF. Когда появятся решения, мы, конечно, сможем оценить их влияние. Мы можем официально и научно измерить его. Мы можем эмпирически измерить это через наши разговоры и взаимодействие с членами сообщества. А затем мы также можем организовать дискуссии, особенно в сообществе ICANN, с именами и цифрами, чтобы увидеть последствия, увидеть движущие силы, увидеть мотивы того, как некоторые из этих технологий могут улучшить (или не улучшить) ситуацию на местах.

ДЖОН КРЕЙН: Хорошо, спасибо, Дэвид.

Мне интересно, сколько людей в этой комнате на самом деле когда-либо участвовали в работе Инженерной проектной группы Интернета?

О, хорошо. Несколько человек. Если вы технический специалист и интересуетесь протоколами, это отличное место для вас. Если вы не гик, вы будете очень смущены, когда окажетесь там. Но для гиков среди нас IETF — это действительно хорошая вещь.

И важно помнить — вы будете шокированы, услышав это — что ICANN не управляет Интернетом. ICANN не занимается разработкой Интернета. Мы не разрабатываем все эти протоколы. Это партнерство. Это сообщество инженеров и людей, использующих Интернет, которые действительно этим

занимаются. Поэтому приятно видеть людей в IETF и на других форумах, а не только здесь.

Думаю, на этом мы закончили? Или есть еще вопросы?

СИРАНУШ ВАРДАНЯН: Мы можем ответить еще на один последний вопрос.

Да, пожалуйста? Афифа, вы ли это?

Да. Афифа, пожалуйста.

АФИФА АББАС (AFIFA ABBAS): Приветствую всех. Это Афифа. Я ментор программы Fellowship. Вот уже два года я являюсь наставником участников программы Fellowship. Один из вопросов, который мне очень часто задают стипендиаты: где в ICANN, с точки зрения новичков в области кибербезопасности, они могут принять участие, где они могут с гордостью сказать, что они принадлежат к этой конкретной кибербезопасности в ICANN? Будучи ментором, мне трудно ответить на этот вопрос, потому что... Итак, если вы можете назвать несколько платформ, чтобы можно было принять участие. Потому что, будучи ментором, я могу сказать, что сейчас набирается огромное количество тех, кто действительно заинтересован в кибербезопасности. И, как вы сказали, программа Fellowship ICANN направлена на привлечение свежей крови. Мы не хотим их потерять, и я также уверен, что ICANN тоже

этого не хочет. Как же мы можем использовать их талант в области кибербезопасности? Спасибо.

ДЖОН КРЕЙН: Хорошо, спасибо, Афифа. Здравствуйте. Всегда приятно видеть возвращающихся участников программы Fellowship, особенно когда они становятся менторами. Отлично. Это интересный вопрос, потому что ICANN не является форумом по кибербезопасности, верно? Мы этим не занимаемся. Но у нас есть трек по безопасности, где все [неразборчиво] в рамках этого трека в повестке дня ICANN.

Если вы ищете совета о том, где можно принять более активное участие в решении вопросов кибербезопасности внутри ICANN, у нас есть комитет под названием SSAC (Консультативный комитет по безопасности и стабильности). Вы можете подать заявление о вступлении. Они ищут в основном опытных специалистов по безопасности. Так что если вы придете как участник программы Fellowship, как опытный специалист по безопасности — потому что вы знаете, у нас есть люди, которые уже давно работают в отрасли в качестве участников программы Fellowship — это то место, на которое стоит обратить внимание.

Мы проводим технические дни. ccNSO проводит серию технических дней, на которых обсуждается много вопросов безопасности.

И конечно, вы всегда можете прийти к нам, и мы поможем вам найти другие области и людей, с которыми можно поговорить.

Многое из того, что важно в ICANN, происходит не только в ходе обсуждения политики. Не забывайте, ICANN — это форум для обсуждения политики. Речь идет о политике в отношении идентификаторов, а это не только безопасность и, конечно, не только кибербезопасность. Но главное, что вы здесь делаете, — это взаимодействуете с людьми в кулуарах и на мероприятиях.

Так что если вы увидели кого-то, с кем вы хотели бы встретиться — не знаю — в вашей области, будь то кибербезопасность или другая область — всегда не стесняйтесь поговорить со своими наставниками или найти сотрудника ICANN или, откровенно говоря, любого человека в сообществе и сказать: «Эй, мне очень интересна тема X, и я нашел этого человека, который, кажется, действительно хорошо разбирается в ней. Не могли бы вы меня представить?», потому что мы все так делаем. Речь идет о совместной работе, по принципу «снизу-вверх», как сообщества. А для этого мы должны сформировать сообщества.

Так что это лучший совет, который я могу вам дать. Есть трек безопасности, так что обратите внимание на это. Обратите внимание на ccTLD, на Tech Day. Поговорите с людьми из SSAC. Поговорите с людьми из RSSAC. Это Консультативный комитет системы корневых серверов. Если вы представляете ccTLD — есть здесь кто-нибудь из ccTLD? Я знаю, что есть несколько человек. Поднимите руки.

Вы занимаетесь безопасностью?

Есть ли вы в списке безопасности ccTLD?

Так что если вы состоите в ccNSO, они тоже занимаются вопросами защиты.

Так что прямого ответа нет, и поэтому вам трудно сказать им об этом. [Отправить нас] к другим людям. Мы проведем с вами индивидуальную беседу и попробуем выяснить, что именно вам подходит. Проблема в том, что вы использовали термин «кибербезопасность», а он означает так много вещей для разных людей. Но мы рады помочь вам.

И я думаю, что Саманех тоже хочет что-то сказать. Вам слово.

САМАНЕХ ТАДЖАЛИ (SAMANEH TAJALI): К тому, что уже сказал Джон, можно добавить, что это интересный вопрос, потому что мы иногда обсуждаем это, но не систематически. У нас также были стажеры, вместе с... Мы делали проекты — маленькие или большие. Мы не говорили об этом внутри компании, но мы... В любом случае, как исследовательские группы, мы реализуем проекты, и мы хотим приветствовать сторонние идеи или операции в наших собственных группах и за их пределами. Так что если ваши подопечные заинтересованы в исследованиях и проектах, пожалуйста, не стесняйтесь присылать их к нам, и мы сможем обсудить и посмотреть, как мы можем это сделать.

СИРАНУШ ВАРДАНЯН: Большое спасибо.

На этом я хотела бы поблагодарить всех наших докладчиков — Мэтта, Саманеха, Дэвида, Джона и Ким — за то, что уделили нам время. Я знаю, что у вас напряженный график, но спасибо, что нашли время и поговорили с нами, с участниками программ Fellowship и NextGen. Они действительно заинтересованы в том, чтобы узнать больше.

И люди здесь, наши участники, вы теперь знаете эти лица. Если вы увидите их в коридорах и захотите задать какие-либо вопросы, пожалуйста, не стесняйтесь подойти к ним и задать свои вопросы.

И завершая эту сессию, я хотела бы сказать: будьте добры друг к другу. Большое спасибо. Объявляю заседание закрытым. Теперь можно остановить запись. Большое спасибо.

[КОНЕЦ СТЕНОГРАММЫ]