ICANN68 | Виртуальный форум по формированию политики — пленарное заседание: DNS и Интернет вещей: возможности, риски и проблемы
Вторник, 23 июня 2020 года — 13:00–14:30 по малайзийскому времени

РИЯ ОТАНЕС: Здравствуйте. Приветствую вас на пленарном заседании, тема которого звучит так: «DNS и Интернет вещей: возможности, риски и проблемы» Меня зовут Рия Отанес (Ria Otanes), я буду координатором удаленного участия для этого заседания.

Пожалуйста, помните о том, что это заседание записывается, и придерживайтесь стандартов ожидаемого поведения ICANN. В ходе этого заседания вопросы или комментарии можно будет зачитывать только в том случае, если они будут подаваться на английском языке через область вопросов и ответов. Это функция, которая вызывается с панели инструментов Zoom. Я буду зачитывать разрешенные вопросы и комментарии во время, определенное председателем или модератором этого заседания. Если вы хотите задать вопрос или внести свой комментарий, поднимите руку. Когда вам предоставится слово, вы получите возможность включить свой микрофон. В таком случае включайте свой микрофон и говорите то, что вы хотели сказать. Для протокола я попрошу вас называть свое имя и язык, на котором вы будете говорить, если это не английский. В ходе этого заседания будет в режиме реального времени вестись стенограмма и перевод. Чтобы вывести на экран стенограмму в реальном времени, нажмите кнопку субтитров на панели инструментов Zoom.

Чтобы нашим переводчикам было проще работать, пожалуйста, говорите четко и не слишком быстро. Чтобы иметь возможность слушать перевод, нужно загрузить специальное приложение для перевода. Более подробные сведения можно найти в информации о заседании в графике конференции, а инструкции приводятся в чате.

И последнее, что я хочу вам напомнить: пользуйтесь раскрывающимися меню в области чата, чтобы переключаться между ответами для всех членов комиссии экспертов и ответами для комиссии экспертов и всех участников, если вы хотите, чтобы ваши комментарии в чате были видны всем присутствующим.

На этом я передаю слово Алехандре Рейносо (Alejandra Reynoso). Алехандра, прошу вас.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Рия.

Всем привет. Меня зовут Алехандра Рейносо. Я работаю в .gt, это ccTLD Гватемалы, и мне выпала честь быть председателем на этом пленарном заседании.

Интернет вещей обещает сделать нашу жизнь проще, а наше общество — безопаснее, разумнее и устойчивее, и все это благодаря десяткам миллиардов подключенных устройств, которые пассивно и автономно считывают данные нашей физической среды и действуют в соответствии с ними. Несмотря на то, что этим Интернет вещей разительно отличается от таких

традиционных интерактивных способов использования Интернета, как электронная почта и веб-сайты, многие устройства Интернета вещей для нахождения необходимых им служб будут использовать систему доменных имен.

Консультативный комитет по безопасности и стабильности, SSAC, недавно опубликовал документ SAC105 — это отчет, в котором обсуждаются возможности, риски и проблемы, связанные с взаимодействием между Интернетом вещей и DNS. Сегодняшнее пленарное заседание позволит придать дополнительное содержание диалогу, который является целью этого документа, в частности за счет того, что члены сообщества, представляющие разные группы интересов, получат возможность обсудить эту тему с экспертами в этой предметной области, а также между собой.

Это пленарное заседание является своего рода продолжением заседания ccNSO по документу SAC105 на конференции в Монреале, в ходе которого особое внимание было уделено вопросу ccTLD.

В рамках этого пленарного заседания перед нами стоят цели лучше понять, как именно Интернет вещей отличается от традиционных интерактивных способов использования Интернета и как он использует систему DNS, разобраться в том, что думают ключевые игроки отрасли DNS и Интернета вещей о взаимодействии между этими двумя экосистемами в том, что касается возможностей, рисков и проблем, а также продвинуться в понимании того, какую роль сообщество ICANN потенциально могло бы играть в этом пространстве.

Следующий слайд, пожалуйста.

Это сегодняшняя повестка дня. Первым у нас будет краткий обзор документа SAC105. Затем у нас будет комиссия экспертов, которые поделятся с нами своими взглядами по этому вопросу. После этого у нас будет оценка коллегами, когда выступающие будут делиться своими мнениями о выступлениях экспертов. А затем мы завершим наше заседание ответами на вопросы аудитории.

Следующий слайд, пожалуйста.

Позвольте мне в двух словах представить вам Кристиана Хессельмана (Cristian Hesselman), который представит нам обзор документа SAC105.

Кристиан занимает пост директора в организации SIDN Labs, это исследовательская группа компании SIDN, оператора национального домена Нидерландов .NL. Она ставит перед собой цель продвинуться в вопросах обеспечения операционной безопасности и отказоустойчивости сквозной передачи данных в Интернете в рамках эмпирических исследований на основе измерений, создания прототипов и оценки эффективности новых систем и инструментов Интернета.

Кристиан также является членом SSAC, он руководил рабочей командой SSAC, которая подготовила этот документ SAC105 «DNS и Интернет вещей: возможности, риски и проблемы».

Кроме того, он занимает должности приглашенного адъюнкт-профессора Университета Твенте в Нидерландах и председателя правления компании NLNetLabs.

Кристиан, вам слово.

КРИСТИАН ХЕССЕЛЬМАН: Хорошо. Большое спасибо, Алехандра.

Итак, для меня большая честь представить вам сегодня краткий обзор документа SAC105, то есть отчета, который SSAC выпустил в июне 2019 года. И, как уже сказала Алехандра, этот документ посвящен взаимодействию между Интернетом вещей, или сокращенно ИВ, и системой DNS, при этом особое внимание уделяется тому, чтобы инициировать и способствовать дальнейшему развитию дискуссии в сообществе ICANN.

Чуть позже в этом году этот отчет также будет опубликован как рецензированный документ в журнале, который называется IEEE Internet Computing.

Следующий слайд, пожалуйста.

Итак, Интернет вещей. В нашем отчете мы использовали определение Интернета вещей, которое было дано Обществом Интернета еще в 2015 году, то есть это такое применение, которое... там сказано, что оно расширяет возможности вычислений и подключения к сетям на различные предметы, устройства, датчики и все то, что обычно не считается

вычислительными устройствами. То есть, по сути, речь идет о том, чтобы подключить к сети все то, о подключении чего раньше вы даже не задумывались.

Отличия от традиционных, так сказать, интерактивных способов использования Интернета, таких как электронная почта и веб-сайты, некоторые из этих отличий таковы. То есть Интернет вещей постоянно считывает характеристики физического пространства и взаимодействует с ним. Это важное различие. Кроме того, чтобы реагировать на изменение этого пространства, он также интерпретирует информацию, которую получает от различных датчиков. Обычно это происходит без ведома пользователя, то есть представьте себе крохотные датчики, встроенные, например, в стены или еще какие-то объекты, с которыми вы взаимодействуете, на самом деле не зная об этом. То есть это то, что специалисты Общества Интернета называют пассивным взаимодействием в отличие от интерактивного взаимодействия, которое имеет место при работе, например, с веб-браузерами и клиентами электронной почты. То есть этих устройств Интернета вещей будет огромное множество. По крайней мере так это прогнозируют многие аналитики рынка. Кто-то говорит о цифрах от 20 до 30 миллиардов таких устройств, которые, так сказать, по сути, работают на заднем плане нашей с вами жизни. Так, что мы их на самом деле не видим. Мы взаимодействуем с ними, не зная о них.

Еще одно отличие — это то, что устройства ИВ обычно гораздо более гетерогенны по сравнению с тем, к чему мы привыкли в

мире ноутбуков и мобильных телефонов. То есть речь идет о разных типах операционных систем. Речь идет о разных аппаратных архитектурах, о разных типах сетевых подключений. То есть это не только Wi-Fi. Это также ZigBee, это также другие типы беспроводных сетей.

Хорошо. И наконец, Интернет вещей также отличается тем, что для устройства ИВ отличаются гораздо более продолжительным сроком службы, возможно, потому, например, что они встраиваются в различные физические структуры, а также они отличаются работой, не требующей вмешательства человека. То есть не нужен никакой администратор этой сети или еще кто-то, кто бы присматривал за этими устройствами. Они там просто работают себе и подключаются к сети, а вы об этом и не подозреваете.

Так что Интернет вещей уже довольно продолжительное время считается такой, как бы сказать, следующей большой инновацией. На самом деле это все уже работает начиная, кажется, с 1990-х годов, тогда это называлось «проникающие вычисления» или как-то так. То есть это были разные названия для примерно одной и той же идеи. Но, как бы то ни было, сейчас мы подходим к такому этапу, когда становится возможным на самом деле развертывать все эти разные устройства, датчики и переключатели, и в результате этого многим кажется... распространено такое мнение, что ИВ сделает наше общество более безопасным, разумным и устойчивым. К примеру, в области интеллектуальных транспортных систем, это интеллектуальная

маршрутизация трафика на территории городов, к примеру, на основе данных от самых разных датчиков, или же это могут быть интеллектуальные энергосистемы или, возможно, умные дома или умные города. Я считаю, что последнее — это более привлекательный пример, это то, что всем нам знакомо в связи со всеми этими технологиями, которые используются в наших домах в наше время.

Хорошо. Так что Интернет вещей, так сказать, это очень многообещающая технология, но есть одна большая проблема, и это безопасность Интернета вещей, и я сейчас об этом тоже скажу.

Следующий слайд, пожалуйста.

Спасибо.

Итак, это пример... Это модель, которую мы используем в... в комитете SSAC для понимания Интернета вещей. То есть вы видите здесь такую сложную картину физических пространств слева, давайте возьмем эту верхнюю часть. Итак, то, что вы видите здесь в левом верхнем углу, — это люди в своих домах, и они взаимодействуют с тем, что мы называем развертыванием Интернета вещей. Это, по сути, вот эта затененная область в центре экрана. А развертывание Интернета вещей состоит из трех компонентов. Один — это устройства Интернета вещей. Второй — это возможности подключения к сетям. А третий — это службы технической инфраструктуры, понимаете?

Вот здесь есть пример с маленькими часами и интеллектуальным дверным замком, когда кто-то подходит к двери, например, человек приближается к двери своего дома, а у него там какой-то умный дверной замок, и вся эта информация о приближении собирается... с помощью умных часов, которые носит этот человек, плюс, к примеру, дверная ручка считывает отпечатки пальцев, и эта информация отправляется через Интернет какой-то удаленной службе, и на основе этой информации эта служба принимает решение о том, нужно ли отпирать дверной замок. Это, разумеется, будет регулироваться какой-то пользовательской политикой.

То есть на этом очень простом примере вы видите, что информация, считываемая верхним устройством, D1, это умные часы, например. Эта информация передается по Интернету удаленной службе, которая затем присылает дверному замку информацию о том, следует ли открывать дверь.

То есть вы видите здесь считывание данных и реагирование на... считывание и реагирование на данные физической среды пользователя, которое происходит прозрачно... без ведома пользователя, да?

То есть пользователи видят только устройства, они видят свои умные часы и свою умную дверную ручку, к примеру, но они не видят всю эту сложную механику, которая за этим стоит.

И одной из частей этой сложной механики является система DNS, потому что, насколько нам известно из прошлых исследований на

эту тему, эти устройства, они... для выполнения своих функций они взаимодействуют со службами в Интернете, да? Так что... и это то, что отличает их от традиционного просмотра веб-страниц, когда вы пользуетесь веб-браузером для получения какой-то информации с веб-сайта или для использования какой-то услуги. Это... в таком сочетании устройства используют службы для выполнения своих функций, понимаете?

То есть, к примеру, в этом конкретном случае эта служба может анализировать данные датчика, поступающие от пользователя, и затем принимать решение о том, следует ли открывать дверь. Понятно?

И в этом взаимодействии DNS играет важную роль, но я не буду вдаваться в детали, потому что после этой презентации Элиот расскажет об этом подробнее.

Хорошо. Я думаю, что на данный момент это самое важное, так что, пожалуйста, следующий слайд.

Хорошо. Итак, этот отчет озаглавлен «DNS и Интернет вещей: возможности, риски и проблемы». У меня есть отдельный слайд для каждого из этих трех компонентов: один для возможностей один для рисков и еще один для проблем. Возможности — это то, о чем мы обычно не говорим в DNS, потому что... в комитете SSAC, потому что мы в первую очередь сосредотачиваем наше внимание на проблемах и рисках, мы должны это делать, но в данном случае мы подумали, что нужно... что это возможность для DNS, потому что это глобальная... глобальная инфраструктура доверия, если

можно так выразиться, которая может помочь усовершенствовать конфиденциальность, безопасность и транспарентность Интернета вещей. Так что мы действительно считаем, что DNS может принести пользу в этом вопросе.

Я здесь перечислил три момента. Подробнее это описано в документе SAC105. Итак, первое — это то, что, на наш взгляд, DNS может снизить риск сбора информации о пользователях, и это благодаря тому, что эти устройства, о которых мы говорили, они взаимодействуют с DNS. Итак, DNS-запросы, если на пути передачи между устройством ИВ и используемой им удаленной службой есть наблюдатель, он может видеть, в зависимости от того, каким образом осуществляется взаимодействие с DNS, кто тот человек, который находится у себя дома, к примеру, какие устройства при этом используются или что... возможно даже, используются ли те или иные устройства, потому что при этом происходит обмен данными с DNS.

И еще одна возможность — это то, что, если вы, проанализировав доменные имена, узнаете, какие устройства ИВ используются, вы можете даже... то есть злоумышленник может попытаться... попытаться установить конкретное устройство ИВ, которое отправляет эти запросы, понимаете? То есть существуют исследования, которые показывают, что многие устройства ИВ подают запросы только в отношении небольшого набора доменных имен, когда обращаются к этим удаленным службам, о которых мы говорили, рассматривая предыдущий слайд. И иногда такие DNS-запросы или используемые в них доменные

имена могут раскрывать информацию о типе устройства, которое их отправляет, понимаете? То есть это, что мы имеем в виду, когда говорим о риске сбора информации о пользователях. И, разумеется, для этого можно шифровать отправляемые такими устройствами ИВ DNS-запросы. Это можно делать, например, посредством таких технологий, как DoH или DoT, в отношении которых ведется много споров.

Еще одна возможность, которую мы предвидим, — это снижения риска перенаправления устройств ИВ на другие удаленные службы. То есть, к примеру, мы видели... в Интернете мы наблюдали концепцию т. н. перехвата маршрута. В результате таких действий трафик направляется в сеть злоумышленников. И это то, что может очень сильно сказаться на Интернете вещей, потому что устройства ИВ в таком случае больше не будут подключаться к своим... к тем службам, к которым они должны подключаться, а вместо этого они будут подключаться к службам злоумышленников. И риск тут заключается в том, что люди передают удаленным службам свои данные... свои конфиденциальные, очень личные данные, а это означает, что удаленные службы смогут даже взаимодействовать с физической средой пользователей, понимаете? То есть это риск.

Мы считаем, что DNS может в этом помочь, потому что, разумеется, у нас есть DNS... DNSSEC, да? То есть это позволяет проверять целостность данных, поступающих из DNS. И в случае перехвата маршрута, для примера, клиенты DNSSEC смогут это

определить, потому что они могут... они это видят, потому что подписи сообщений DNSSEC не подтверждаются.

И еще одна возможность, которую мы видим, — это то, что... регистраторы получат возможность обеспечивать многофакторную проверку подлинности. Сокращенно многофакторная проверка подлинности называется MFA, от multifactor authentication.

К примеру, они смогут более надежно защитить доменные имена, используемые устройствами ИВ, задействуя для этого различные факторы, возможно, даже сканирование отпечатков пальцев. Понятно? То есть это две возможности, которые мы видим в том, чтобы снизить риск перенаправления устройств ИВ на поддельные службы, используемые злоумышленниками.

И еще, наконец, мы видим возможность обеспечить большее понимание того, какие службы и резолверы используются устройствами ИВ. Чаще всего люди, взаимодействующие с устройствами ИВ, на самом деле не знают, какого рода информация передается и каким именно службам в Интернете. А если, скажем, сделать DNS-запросы, которые передают устройства пользователей, если сделать их видимыми для конечных пользователей, это поможет им лучше понимать такое взаимодействие, правда?

То есть в предыдущем примере вы бы увидели... вы бы могли видеть, что ваши часы, например, передают информацию удаленной службе в Интернете. Понятно?

Следующий слайд, пожалуйста.

То есть это такая обратная сторона медали, эти риски. Итак, наверное, мне следует рассказать только о... я попытаюсь немного это сократить. Итак, самый большой риск, который мы видим, — это то, что использование Интернета вещей может привести к масштабным атакам DDOS на DNS, понимаете? То есть когда мы наблюдали это раньше, разумеется, это печально известные атаки DDOS в 2016 году на оператора DNS Dyn. Но мы также наблюдали формирование в Интернете и других ботнетов с использованием устройств ИВ, и они могут очень быстро наращивать свои размеры. Потенциально они могут также начать использовать открытые резолверы, чтобы перенаправлять трафик атак DDOS с них на системы жертв, или даже мультиплицировать трафик, направляемый на жертв атак.

Еще один риск — это то, что мы называем программированием, недружественным к DNS, когда DNS используется примитивным способом, к примеру, у нас были... несколько лет назад у нас был случай, когда приложение для iPhone создавало случайные DNS-запросы, вынуждавшие резолверы сбрасывать кэш, потому что они не могли кэшировать данные, а зеркала заканчивались.

Следующий слайд, пожалуйста.

Итак, мы видели... мы обсудили модель Интернета вещей, которую мы разработали в SSAC. Мы обсудили возможности, мы обсудили риски. Следующий вопрос у нас звучит так: что нам нужно делать, чтобы воспользоваться этими возможностями и учесть эти риски?

И мы придумали насколько задач для отраслей DNS и Интернета вещей, которые мы записали здесь. Это на самом деле несколько выходит за пределы круга вопросов SSAC, потому что мы считаем, что определенную роль здесь должно сыграть и сообщество Интернета вещей.

Итак, первое — это разработка для этих устройств ИВ библиотеки безопасности, в которой были бы реализованы те функции, о которых мы только что говорили, когда обсуждали слайд, посвященный возможностям. То есть там должна быть проверка DNSSEC, к примеру, поддержка DoH/DoT, а также функции, которые делали бы DNS-запросы видимыми для конечных пользователей каким-то удобным и понятным способом.

Еще одну задачу мы видим в том, что касается обучения. То есть это обучение специалистов в области Интернета вещей, чтобы они понимали, что такое DNS и в чем заключаются функции безопасности, что нужно делать, чтобы пользоваться ими, и наоборот, обучение специалистов в области DNS тому, как работает Интернет вещей, и, возможно, тому, как Интернет вещей изменит использование доменов, что это, возможно, потребует обеспечить различного рода функции для Интернета вещей... для регистрации доменных имен и обеспечения их безопасности.

Последние, возможно, немного сложноваты, это такие сложные сложности. Итак, первое — это сотрудничество с группой операторов DNS для обмена тем, что мы называем отпечатками пальцев DDOS. То есть это были бы такие сводные данные об

атаках DDOS, которым подвергались эти операторы DNS. Тогда они бы делились этой информацией друг с другом, чтобы повысить свою готовность к атакам.

Эти операторы DNS могли бы даже попытаться делиться друг с другом своими ресурсами для противодействия атакам на DNS. Ну, например, мощностями для очистки трафика. И мы также предвидим, что системы на границах сетей будут играть определенную роль в том, что касается защиты от атак DDOS и вторжений. Вторжений в том, что касается устройств.

И наконец, это мы так немного мечтательно, но было бы очень неплохо, на наш взгляд, предусмотреть какую-то систему, которая позволяла бы измерять эволюцию Интернета вещей и видеть, как он растет и как он использует DNS.

Вот такие у меня слайды, Алехандра.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Кристиан.

Сейчас мы продолжим с нашей комиссией экспертов, которые поделятся с нами своим видением этой проблемы в следующем порядке. Сначала Элиот, затем Лизе, и третьим будет Кристиан.

Позвольте мне сначала представить вам Элиота Лира (Eliot Lear) и Лизе Фур (Lise Fuhr). Элиот Лир работает главным инженером компании Cisco Systems в области безопасности Интернета вещей и основное внимание в своей работе уделяет проблемам

взаимодействия между устройствами и сетью. Элиот настоящий ветеран интернет-сообщества, он участвовал в работе сообщества IETF начиная с 1998 года, был автором ряда документов RFC и членом Совета по архитектуре Интернета, а также руководил участием IETF в реструктуризации ICANN во время передачи координирующей роли в исполнении функций IANA. Он также занимал руководящие должности в МСЭ. Элиот живет в Швейцарии.

Лизе Фур занимает должность генерального директора Европейской ассоциации операторов сетей связи общего пользования, ETNO, с января 2016 года. Она руководит всей деятельностью ETNO и выполняет функции главного представителя ассоциации во внешних сношениях.

Она также представляет ассоциацию в качестве члена правления и члена административного комитета Европейской организации кибербезопасности. В мае 2019 года Лизе была снова назначена членом правления регистратуры доменов общественного характера Общества Интернета на трехлетний срок.

За плечами Лизе более чем 20 лет опыта работы в отрасли телекоммуникаций. Ее карьера началась в министерстве науки, технологий и инноваций Дании, где она подготовила и внедрила нормы, регулирующие работу рынка связи. После этого она работала в различных компаниях-операторах связи и сетей, где руководила группами специалистов, которые занимались проблемами связности устройств и мобильных устройств...

извините, мобильных сетей, а также сотрудничества в рамках отрасли.

Элиот, вам слово.

ЭЛИОТ ЛИР: Большое спасибо, Алехандра.

Следующий слайд, пожалуйста.

Я хочу рассказать вам историю о печи. Это печь. Она подключается к Интернету. Она поддерживает технологию Интернета вещей. Моя двоюродная сестра купила и установила у себя такую печь, а спустя какое-то время печь прислала ей сообщение в 5:30 утра с напоминанием о том, что ее нужно почистить. Лично я считаю, что это вполне себе отказ в обслуживании. Это так задумано, она так и должна работать.

Просто моя двоюродная сестра не знала, что для того, чтобы это все работало, это устройство оснащено множеством разных компонентов. В этой печи есть не только нагревательный элемент и термостат, соответствующая изоляция и все остальное, что должно быть у печи, но также приемопередатчик, центральный процессор, какая-то память, программные переключатели и дисплей.

Это представляет угрозу. Я хочу сказать, что если устройство оснащено этими компонентами, то его можно атаковать. А что можно сделать в рамках такой атаки? Ну, если получится, можно,

наверное, сжечь утку, которая там готовится, или, в худшем случае, можно создать такую координированную атаку, когда все печи включатся в неудобное время. Скажем, если в регионе энергосети работают на пределе из-за жаркой погоды, когда у всех включены кондиционеры. И тут разом включатся все печи: это может привести к аварийному отключению энергосети.

Более того, значительная часть программного стека этой печи используется другими устройствами, это могут быть кондиционеры, печи, радиоприемники, дверные звонки. Так что включить одновременно можно было бы сразу множество разных устройств, что вызвало бы огромный скачок потребления электроэнергии. Поэтому для такой печи необходимо предусмотреть какую-то защиту.

Следующий слайд, пожалуйста.

Следующий слайд, пожалуйста.

Чтобы эта печь работала — она же не напрямую присылала эти сообщения. Здесь у нас картина Интернета, замечательная картина Интернета, созданная не так давно Кейси и ее группой.

Следующий слайд, пожалуйста.

Чтобы это сделать, эта печь на самом деле связывалась с устройствами в облаке. Она делала это так же, как и дверной звонок. То есть это распространенный шаблон поведения.

На один назад, пожалуйста. Спасибо.

И сообщение на ее iPhone на самом деле прислали именно облачные устройства. И это распространенный шаблон.

Чтобы связываться с облаком, эти устройства должны использовать систему доменных имен. У них облачная оконечная точка. Это что-то вроде cloud.example.com. Таким образом они связываются.

А чтобы они вообще могли передавать что-то в Интернет, эти данные должны быть направлены по маршруту, который указывает ближайший маршрутизатор.

Для этой печи, как и для того дверного звонка, речь идет о сети WiFi. Но это можно сделать множеством других способов. Но значительная часть таких данных действительно передается через домашнюю сеть, через ее маршрутизатор.

Следующий слайд, пожалуйста.

Как это работает? Вы получаете, к примеру, запрос адреса, который нужен этой печи — следующий слайд, пожалуйста — это запрос адреса домена ovencloud.example.com, и в ответ выдается соответствующий IP-адрес. А IP-адрес тоже приходит с какого-то конкретного адреса. Теперь давайте вспомним то, о чем говорил Кристиан. Этих устройств существует около 20 миллиардов. У нас в Интернете есть множество устройств, но печи нужно связаться только со своей оконечной точкой в облаке, возможно, с несколькими оконечными точками, возможно, с несколькими

устройствами дома, а связываться со всеми остальными ей не нужно.

Так что если этот... этот домашний маршрутизатор сможет выдать какую-то контрольную точку, то такая контрольная точка позволит ограничить поверхность атаки этой печи. Это означает, что даже если в печи будет какая-то ошибка или уязвимость, такая контрольная точка сможет защитить ее от широкомасштабных атак. Значит ли это, что производителю печи не нужно поставлять обновления программного обеспечения для исправления ошибок? Разумеется, нет. По-прежнему... поверхность угрозы все-таки существует, даже при всех этих мерах защиты, просто сеть помогает уменьшить возможности такой угрозы.

Следующий слайд, пожалуйста.

То есть вот данные, которые передаются на устройство, на облачную оконечную точку, адрес которой был выдан системой DNS. Для работы контрольной точки запрос имени от печи и ответ на него должны проходить через нее. Это означает, что если DNS-запрос будет зашифрован и контрольная точка не будет об этом знать, она не сможет обеспечить защиту и сократить поверхность угрозы.

Следующий слайд, пожалуйста. И, разумеется, то же самое будет и с дверным звонком, и с множеством других потребительских устройств.

В мире промышленного оборудования все выглядит несколько иначе. Сегодня я в основном сосредоточусь на том, что мы могли бы наблюдать в случае с потребительскими устройствами. Мы видим множество различных облачных оконечных точек, которые используются множеством различных устройств.

Следующий слайд, пожалуйста.

Что это все означает? Это означает, что нам нужно... что шифровать данные можно. Есть веские основания шифровать DNS-запросы, Кристиан многие из них упомянул. Однако если контрольная точка... если маршрутизатор вашей сети, который должен сократить поверхность угрозы, сам не может получить доступ к запросу, если он не авторизован каким-то образом для просмотра передаваемых данных в том, что... как запроса, так и ответа на него, в таком случае этот маршрутизатор не сможет обеспечить необходимую защиту. То есть такая защита невозможна без этой связки между DNS и маршрутизатором. И эта работа была стандартизирована в IETF в качестве одного из средств обеспечения такой защиты.

То есть мы не говорим, что шифровать нельзя. Совсем наоборот. Мы говорим, что шифровать нужно. Однако при этом нужно сделать так, чтобы шифрование было доступно некоему компоненту, который имеет полномочия обеспечивать определенную (неразборчиво).

Кажется, это мой последний слайд.

Алехандра?

АЛЕХАНДРА РЕЙНОСО: Спасибо, Элиот.

Сейчас у нас Лизе.

ЛИЗЕ ФУР: Спасибо. И приветствую всех. Я представлю здесь взгляд несколько под иным углом, поскольку я представляю сторону операторов связи, интернет-провайдеров.

Следующий слайд, пожалуйста.

Итак, если... мое выступление будет посвящено тому, что делает тему связи 5G и Интернета вещей такой интересной. Я немного расскажу о тех новых возможностях, которые открывает перед нами связь 5G, а также я хочу затронуть некоторые опасения, которые высказываются в адрес 5G и DNS, и рассказать о том, как мы видим то направление, в котором движется мир сейчас в связи с 5G, Интернетом вещей и DNS.

Следующий слайд, пожалуйста.

Итак, если мы посмотрим... поднимем тему Интернета вещей, почему это так интересно в том, как это соотносится с 5G? Это потому, что мы как операторы связи видим, что 5G, а это на самом деле смесь из стационарных и мобильных сетей, это не просто обновление технологии 4G. Это в гораздо большей степени конвергентная технология. То есть мы видим, что это на самом деле будет способствовать и станет важной составляющей Интернета вещей.

Вот здесь вы можете видеть цифры, они относятся только к Интернету вещей на основе мобильной связи, и это может быть даже очень незначительная цифра, здесь видно, что в 2018 году мы наблюдали 140 мобильных подключений... подключений Интернета вещей, а к 2026 году мы ожидаем почти 740 миллионов.

Что такого нового и интересного будет в 5G? Будет ли это узкополосная связь для Интернета вещей, а еще, конечно же, там будут определенные... усовершенствования в том, что касается MTC, и это будет следующая... развитие того, что уже есть в связи четвертого поколения, то есть 4G.

А если мы взглянем на 5G, то это... это будет набор служб, которые будут использовать наработки, уже существующие в технологиях второго, третьего и четвертого поколения, то есть 4G, которые уже сейчас поддерживают Интернет вещей. Однако новый Интернет вещей будет в гораздо большей степени основан на IP-инфраструктуре, и еще в большей степени на DNS-инфраструктуре.

То есть то, что мы наблюдаем прямо сейчас, это не то, что называется Интернетом вещей, потому что в этом используются IP-технологии, но в гораздо большей степени используются другие службы. И мы ожидаем, что в сетях 5G Интернет вещей будет использоваться не так, как он используется сегодня. Мы считаем, что такое использование будет оптимальнее, безопаснее.

И если мы посмотрим на то, что сказано на этом слайде, то Интернет вещей вообще и Интернет вещей в сетях 5G не возникает сам по себе в вакууме. Он на самом деле основывается

на широком портфеле услуг. А технологии DNS и IP будут в общем объединять это все.

Следующий слайд, пожалуйста.

И если мы посмотрим на наследование мобильных сетей 5G и DNS, то сети 5G не станут сразу же совершенно отдельными сетями 5G. В настоящее время мы видим множество сетей 5G, которые создаются поверх инфраструктуры 4G. То есть мы видим сети 4G на оборудовании 5G, но это еще не полноценные сети 5G.

И использование DNS и доменных имен в таких базовых мобильных системах не является преобладающим, то есть мы во многом используем DNS, но пока это ограничено.

И мы действительно видим, конечно же, исключения в маршрутизации, полагающиеся на DNS, одним из таких случаев является технология VoLTE. Но для чего у нас в мобильных системах используются доменные имена? Мы видим, что взаимодействие между доменными имена в настоящее время ограничено, это тянется еще от старых идентификаторов, а мобильный доступ в Интернет неспецифический. Ну, то есть это для мобильных устройств.

То есть в использовании сетей 4G и 5G в том, что касается DNS, нет ничего нового, то есть в сетях 5G DNS используется так же, как и в сетях 4G. Следующий слайд, пожалуйста.

Так что же интересного в технологиях 5G и почему они интереснее, чем 4G? Потому, что, как я уже сказала, это в гораздо

большей степени конвергентные сети. Это виртуализированные сети, которые по сравнению с 4G в большей степени будут использовать программные компоненты, и в меньшей — аппаратные. Это будут гораздо более гибкие сети. И, как мы говорим, они будут основываться на протоколе IP. И хотя на самом деле управлять адресами IPv6 сложно, потому что они очень длинные, мы предвидим, что DNS будет использоваться для этого очень широко из-за структуры IPv6.

Мы также видим, что взаимодействие между доменами будет изначально основано на IP-технологиях, и мы будем постепенно переходить к использованию протокола IP и доменных имен в управлении сетями.

Так что это... в Европе межсетевое взаимодействие у нас по-прежнему в значительной степени основывается на коммутации, однако мы считаем, что с приходом сетей 5G у нас станет больше межсетевого взаимодействия на основе протокола IP. То есть эволюция движется в этом направлении, если говорить об эксплуатации сетей 5G.

Следующий слайд, пожалуйста.

Если мы посмотрим на то, каким образом будет реализовано использование доменных имен, по сути, это будет прозрачно для пользователей в том смысле, что пользователи не будут видеть, как мы используем DNS. То есть то, как мы работаем с нашими сетями, это в большей степени техническая составляющая, и это будет встраиваться в устройства, то есть использование не будет

привязано к доменному имени. То есть имена не будут какой-то очень важной составляющей такого использования, а технология DNS, разумеется, будет.

И, еще раз, если говорить об Интернете вещей и о том, как он будет реализован, это... это ключевой момент, потому что именно реализация будет определять конфигурацию. Так что при том, что мы видим, что технология 5G не... мы не думаем, что технология 5G станет каким-то значительным стимулом для регистрации множества доменных имен второго уровня, но мы на самом деле считаем, что это будет определяться гораздо большим количеством поддоменов. То есть мы не ожидаем какого-то скачка в использовании доменных имен, потому что будет использоваться больше поддоменов. И, опять же, разрешение многих из них будет осуществляться не в Интернете, а в каких-то интрасетях или междоменных пространствах.

Следующий слайд, пожалуйста.

Так почему же мы считаем, что сети 5G принесут пользу Интернету вещей и Интернет... и DNS? Первое и главное — мы считаем, что на уровне ядра сети у нас будет, как я уже сказала, гораздо больше программных решений, а это позволит обеспечить гораздо большую гибкость и удобство в реализации межмашинного взаимодействия в узкополосном диапазоне. Благодаря 5G нам станет проще создавать определения сетей. А с точки зрения безопасности для нас будет крайне важно использовать сегментирование сетей. Сегментирование сетей —

это когда мы будем определять для конкретного вида использования какие-то части сетей. К примеру, автоматизация автотранспорта, а это огромная сфера применения Интернета вещей, потребует использования связи с крайне малым уровнем задержки. То есть будет важно использовать какой-то один вид служб для автоматизации автотранспорта.

Кроме того, мы считаем, что использование искусственного интеллекта на самом деле позволит нам использовать для наших сетей открытые стандарты, как для усовершенствования их, так и для поиска каких-либо возможных угроз или проблем в наших сетях. Мы считаем, что искусственный интеллект позволит нам работать гораздо быстрее и лучше находить проблемы.

Итак, вернемся к проблемам, следующий слайд, пожалуйста.

Если мы посмотрим на то, что нам представляется проблемами, а также на способы их решения, на наш взгляд, сегментирование сетей — это очень удачная технология. Высказывались опасения того, что это приведет к фрагментации Интернета. Мы не видим в связи с этим вообще никаких проблем. Мы считаем, что это будет как VPN, и это еще... эти службы гораздо более ориентированы на конечных пользователей и не приведут к какой бы то ни было фрагментации Интернета.

Если мы посмотрим на проблему предотвращения совпадения доменных имен, мы используем общедоступные домены и не рассматриваем это как проблему. Если будет какой-то домен, который мы будем использовать для внутренней маршрутизации,

то это будет общедоступный домен и никаких конфликтов имен при этом не будет.

Если говорить о стороне DNSSEC, а это важный компонент, то это будет возможность. Это не стандарт... это не обязательный стандарт для сетей 5G на данный момент. Мы не видели ничего, что обуславливало бы необходимость использования DNSSEC в сетях 5G в качестве стандарта, но использоваться эта технология будет.

Опять же, если говорить об атаках типа «отказ в обслуживании», то есть DDOS-атаках, и ботнетах, то в сетях 5G мы, конечно же, сможем с этим справиться. Однако существует тенденция к использованию шифрования. И если мы должны будем отслеживать такие атаки, то нам нужно будет видеть трафик.

Так что если говорить об атаках типа «отказ в обслуживании», если мы должны стать активными участниками такой защиты, то нам нужно видеть трафик.

Следующий слайд, пожалуйста.

В каком направлении мы будем двигаться? В том, что касается стандартизации 5G, все еще остается множество открытых вопросов. Мы пока еще только создаем сети 5G. И, как я уже сказала, мы пока еще не видели много отдельных сетей 5G. То есть пока мы создаем сети 4G с 5G-составляющей.

Инфраструктура стоит дорого. Я вижу это так, что технологии 5G пока не являются в полной мере самодостаточными. Сети 5G

пока еще не в ближайшем будущем, потому что, если говорить о коммерческом использовании (неразборчиво), это очень дорогие сети.

И последнее — мы на самом деле наблюдали этот кризис, связанный с COVID, и это ужасный кризис для всех нас, но мы видим по всему миру мощный акцент на необходимости цифровизации. Мы видели сильный акцент на безопасности.

То есть с такой точки зрения мы увидели, что растет понимание важности инфраструктуры, понимание важности безопасности, а также мы видели рост использования наших сетей. Так что мы считаем, что в будущем мы будем меньше путешествовать. Мы здесь сегодня. Это очень хороший пример — никто из нас не поехал на какую-то конференцию ICANN, вместо этого мы проводим ее в удаленном режиме.

И в том, что касается Интернета вещей, что это будет, разумеется, один из результатов этого кризиса, переход к удаленному мониторингу и более широкому использованию Интернета вещей.

Это была моя часть. Спасибо.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Лизе.

Теперь у нас Кристиан.

КРИСТИАН ХЕССЕЛЬМАН: Да. Спасибо, Алехандра.

Я, по сути, просто перевоплощусь. Раньше... перед этим я выступал как представитель SSAC. Сейчас я буду выступать как представитель домена .NL, который... следующий слайд, пожалуйста.

Итак, .NL — это регистратура национального домена Нидерландов. Мы небольшая страна в Европе. Однако мы можем начать с того, что на прошлой неделе мы превысили отметку в 6 миллионов доменных имен. То есть это было довольно круто, мы это отмечали в сети.

Но из того, что мы делаем, важно... одна из важных задач, стоящих перед нами, — мы стремимся повысить безопасность и отказоустойчивость Интернета, как вы можете видеть на этом слайде. И именно поэтому несколько лет тому назад мы решили начать работать конкретно над Интернетом вещей, чтобы учесть те сложности, о которых я говорил ранее, в той части нашего доклада, в которой мы обсуждали возможности, риски и проблемы.

А причина, по которой мы взялись за это, указана на следующем слайде. Это, по сути, атака на Dyn, когда в 2016 году один из операторов DNS был атакован ботнетом, который генерировал большие объемы трафика. Этот ботнет состоял из сотен тысяч зараженных устройств ИВ, которые все одновременно направляли в адрес выбранной жертвы большие объемы трафика. Это вызвало перебои в работе популярных служб, таких как Twitter, Spotify и многие другие.

И когда мы это увидели, мы подумали: «Мы оператор DNS. Мы обеспечиваем работу критически важной инфраструктуры Нидерландов, а также Интернета в целом, поэтому нам нужно что-то с этим делать». И именно тогда мы начали работу над прототипом системы SPIN. Аббревиатура SPIN означает безопасность и конфиденциальность домашних сетей (Security and Privacy in In-home Networks).

Задача этой системы, по сути, заключается в мониторинге... то есть вы размещаете устройство в домашней сети или расширяете возможности своего домашнего шлюза, — это то, о чем говорил Элиот, — за счет дополнительной функциональности, связанной с безопасностью. И эта функциональность затем позволяет вести мониторинг вашей локальной сети на предмет трафика атак DDOS, к примеру, то есть определять признаки того, что одно из ваших домашних устройств Интернета вещей может быть инфицировано ботнетом, например, и участвовать в одной из таких масштабных атак DDOS.

И тогда мы бы попытались временно отключить такое устройство от Интернета, чтобы защитить инфраструктуру Интернета от таких атак DDOS. То есть это такой брандмауэр наоборот, если можно так сказать.

То есть это пример того, что мы создали в лаборатории SIDN. В настоящее время эта система находится на стадии прототипа, хотя в прошлом году мы как бы вложились в это программное обеспечение, чтобы вывести его на уровень рабочей системы,

потому что мы хотели помочь интернет-провайдерам и производителям потребительского оборудования, которые также могли бы использовать эти функции в своих устройствах. Однако это оказалось гораздо сложнее, чем мы думали, потому что эта экосистема отличается от привычной нам экосистемы DNS.

Кроме того, есть... это другая бизнес-экосистема, так сказать. То есть, к примеру, интернет-провайдеры, по крайней мере те, с которыми мы говорили, они испытывают сложности с пониманием того, насколько далеко им следует заходить, помогая своим клиентам решать проблемы с безопасностью устройств Интернета вещей, которые они не сертифицировали. То есть они как бы не очень этого хотят, потому что такого рода дополнительные услуги создают нагрузку на их службы поддержки, к примеру, что приводит к дополнительным затратам. То есть это как бы один из факторов, которые затрудняют развертывание такого рода систем.

А еще один фактор — это то, что производители оборудования, они, по сути... они, по сути, добавляют эти функции в том случае, если их просят об этом их клиенты, то есть интернет-провайдеры. То есть тут тоже получается замкнутый круг.

Но мы знаем, что это важная проблема, потому что если взглянуть на... по крайней мере в Европе, если вы посмотрите на Национальный регулирующий орган в области телекоммуникаций Нидерландов, у него есть конкретная программа, посвященная безопасности Интернета вещей. И в европейских странах есть

также инициативы... когда различные регуляторы отрасли телекоммуникаций из разных стран Европы пытаются расширить действие директивы о радиооборудовании, а это наш нормативный документ для любого устройства, которое оснащено... которое осуществляет передачу радиосигнала, и они пытаются расширить эти спецификации и дополнить их какими-то базовыми требованиями к безопасности Интернета вещей. То есть это указывает на то, что это важная проблема с точки зрения общественных интересов, если можно так выразиться. Однако в отрасли все еще не все подключились к этим усилиям, особенно в мире интернет-провайдеров. В мире тех, кто обеспечивает подключение, я бы так сказал.

Следующий слайд, пожалуйста.

Программное обеспечение, которое вы сейчас видели, основано на открытом программном коде. Вы не видели программное обеспечение. Вы видели рисунок. URL-адрес указан внизу, если вы захотите его себе загрузить.

Еще один пример того прототипа, который мы разработали, — это возросшая транспарентность Интернета вещей. Вы, наверное, помните, я раньше говорил о возможности для DNS визуализировать DNS-запросы для пользователей так, чтобы это было понятно и удобно. И для иллюстрации этой идеи мы разработали прототип. Это то, что вы видите здесь на экране.

Вот эти серые кружки — это, по сути, устройства в сети. Вот этот наверху, наверное, телефон, потому что он подключается ко множеству устройств.

А синие и зеленые фигуры — это, по сути, удаленные службы, к которым эти устройства подключаются. Это снимок экрана.

А на самом деле это приложение очень динамичное. Вы видите... на самом деле вы видите взаимодействие с удаленные службами, они всплывают, когда происходит обмен данными. То есть это основано на DNS-запросах.

И мне следует добавить, что SPIN — это решение, обеспечивающее конфиденциальность, потому что все измерения и анализ остаются в домашней сети. То есть они не передаются в облачные службы или еще что-то такое.

Хорошо. Итак, это были два примера, так сказать, систем, с помощью которых мы пытаемся решить те проблемы, о которых мы говорили в отчете SSAC.

И у меня есть еще один пример, он на следующем слайде.

И этот последний пример, он на самом деле о том, что Общество Интернета пару лет назад называло «кооперативной безопасностью». То есть это когда множество организаций вместе работают над обеспечением безопасности Интернета, что на самом деле жизненно важно для Интернета, потому что Интернет сам по себе является одной большой средой сотрудничества. Так

что если вы хотите обеспечить его безопасность, это нужно сделать вместе.

И один из примеров того, в чем мы участвуем, это то, что вы видите здесь. Это называется «центр обмена информацией об атаках DDOS». И его назначение... это в настоящее время такая централизованная система, которая позволяет участникам обмениваться сводными данными атак DDOS, с которыми они сталкивались в своих системах. То есть к ним поступает входящий трафик. Они создают отпечаток пальцев этого трафика, а затем они делятся им с другими операторами, которые входят в эту группу, чтобы эти операторы знали, что... имела место атака такого рода, чтобы они могли подготовить свою инфраструктуру на тот случай, если впоследствии такая атака будет осуществляться уже на них самих.

То есть это такие упреждающие действия. Для жертвы атаки это уже слишком поздно. Это по-прежнему реагирование по факту. А для других в этой группе это проактивные действия, потому что они получают больше информации об атаках DDOS, и это может произойти с другими поставщиками услуг.

То есть это, по сути, такой информационный уровень, который вы можете добавить поверх своей инфраструктуры противодействия атакам DDOS. Это не заменяет ее. Это дополнительная система... распределенная система, которая добавляется поверх уже существующей.

Над ее пилотной версией мы работаем сейчас в Нидерландах. Есть еще веб-сайт, который я забыл упомянуть, он называется nomoreddos.org. Зайдите и посмотрите, что это. Это такой блог, в котором публикуется дополнительная информация.

Мы в настоящее время изучаем... мы сейчас делаем для Нидерландов пилотный проект, который является частью европейского проекта CONCORDIA, посвященного кибербезопасности в общем. Однако есть... четверть этого проекта на самом деле посвящена центрам обмена информацией об атаках DDOS.

И мы считаем, что... мы сейчас организовали центр обмена информацией об атаках DDOS на национальном уровне. Это значит, что его членами являются организации из Нидерландов, это органы власти, интернет-провайдеры, точки обмена интернет-трафиком, регистратуры и многие другие организации. Банки, например.

Это можно также организовать по-другому. Можно представить себе центр обмена информацией об атаках DDOS для отрасли DNS, к примеру, в рамках которого операторы DNS на уровне регистратур и, возможно, на уровне регистраторов будут сотрудничать с целью обмена информацией об атаках DDOS.

То есть это, по сути, три примера, которые я хотел привести с точки зрения регистратуры .NL, и мы надеемся, что это поможет в решении этих... поможет защититься от тих рисков и воспользоваться теми возможностями, о которых мы говорили в отчете SSAC.

Спасибо.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Кристиан.

Следующий слайд, пожалуйста.

А сейчас пора дать слово рецензентам. Встречайте наших рецензентов. У нас есть Филипп Фукар (Philippe Fouquart). Он представляет группу интересов интернет-провайдеров и провайдеров связи, ISPCP. Филипп — старший эксперт по вопросам имен, номеров и адресов в компании Orange Labs Networks. Начиная с 2001 года он руководил в Orange Labs деятельностью, связанной с именами, номерами и адресами, в рамках разработки архитектуры сетей группы Orange и предоставления технической поддержки в этой сфере бизнес-подразделениям группы по всему миру.

Рафик Даммак (Rafik Dammak) — специалист в области компьютерных наук, который после окончания Токийского университета по специальности прикладных компьютерных наук живет в Японии. Он занимается вопросами гражданского общества и проблемами управления Интернетом с 2007 года и принял участие в качестве докладчика или организатора семинаров в нескольких Форумах по управлению Интернетом, а также других конференциях, посвященных проблемам Интернета.

Основные его интересы — это процессы разработки политики ICANN, в которых он принимал участие в разных ролях как член группы интересов некоммерческих пользователей (NCUC) и группы некоммерческих заинтересованных сторон (NCSG),

а также повышение осведомленности о проблемах управления Интернетом в регионе Ближнего Востока и Северной Африки.

Кимберли «Кей Си» Клаффи (Kimberly KC Claffy) — директор центра прикладного анализа интернет-данных при Калифорнийском университете в Сан-Диего. В 2017 году она стала лауреатом премии Jonathan B. Postel Service Award, а в 2019 году была включена в Зал славы Интернета. Она также занимает должность адъюнкт-профессора на факультете компьютерных наук Калифорнийского университета в Сан-Диего. Как исследователь она интересуется проблемами топологии Интернета, маршрутизации, безопасности, экономики и будущего архитектуры и политики Интернета. В 2003 году она стала членом комитета SSAC ICANN. Обладает степенью доктора философии в области компьютерных наук Калифорнийского университета в Сан-Диего.

Итак, рецензенты, вам слово.

Мы можем начать с Филиппа.

ФИЛИПП ФУКАР: Спасибо, Алехандра. Вы меня слышите?

АЛЕХАНДРА РЕЙНОСО: Да, замечательно.

ФИЛИПП ФУКАР: Спасибо вам и спасибо всем членам комиссии. Итак, несколько выводов и, возможно, один комментарий с моей стороны. Элиот представил сценарии использования, в которых Интернет вещей сводится к устройствам, работающим с некоей системой, а не взаимодействующим друг с другом. Я так понимаю, что предлагается, чтобы в локальной сети был шлюз под управлением Интернета вещей и чтобы он мог видеть как исходящие DNS-запросы, так и ответы на них, мотивируя это тем, что в таком случае можно было бы фильтровать поступающий трафик, что позволило бы сократить количество угроз безопасности.

Лизе, вы проводите различие между двумя измерениями мобильных сетей 5G, когда одно — это Интернет вещей в мобильных сетях, а другое — применение Интернета вещей как услуг, предлагаемых оператором. И вы сказали, что 5G и сегментация сетей — это не угроза единому Интернету и единой системе DNS (неразборчиво). И что существуют архитектуры DNS, которые уже используются в мобильных сетях, и они отличаются от той системы DNS, которую мы видим в Интернете. То есть здесь ничего нового.

И наконец, Кристиан рассказал о пилотной концепции DNS-шлюза Интернета вещей, подразумевающей мониторинг исходящего трафика DNS в системе SPIN лаборатории SIDN, что, в частности, было бы полезно для защиты от атак на DNS типа «отказ в обслуживании».

То есть это то, что я понял из того, что вы говорили.

У меня есть один комментарий или вопрос, касающийся проблем. Учитывая, что Интернет вещей — это сложная экосистема разных действующих лиц, которые могут не участвовать в работе этой организации, а также регуляторов, отвечающих, к примеру, за определение стандартов, тут всегда возникает такой очень общий вопрос о том, каким образом вы будете способствовать или обеспечивать соблюдение правил практической деятельности в том, что касается целей этого проекта в общем или же DNS в частности. И каким образом вы будете взаимодействовать с... с этим сообществом действующих лиц.

Так что это, возможно, вопрос к нашим экспертам или в качестве пищи для раздумий, я бы хотел больше узнать о том... каково ваше место в этой экосистеме, кто вы в ней — оператор, регистратура или поставщик. Как мы можем связаться или как вы можете связаться с этим сообществом производителей устройств для продвижения этих практических правил.

Спасибо. Опять слово вам, Алехандра.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Филипп.

Что касается ваших вопросов, то я думаю, что наши эксперты должны еще немного над ними подумать, а мы могли бы тем временем перейти к другим рецензентам, а потом, в конце, мы вернемся к вашим вопросам.

Сейчас мы можем послушать Рафика.

РАФИК ДАММАК: Хорошо. Спасибо, Алехандра, и спасибо нашим экспертам за их доклады.

Я тоже сделал для себя несколько выводов и как бы пытаюсь понять, как далеко это заходит.

То есть я считаю, что это один из важных вопросов — кажется, это довольно далеко выходит за пределы полномочий ICANN и SSAC, но из-за того, что в этой технологии определенную роль играет DNS, или за счет того, что эта экосистема может использоваться в Интернете вещей, это делает эту тему интересной для нас, но мне показалось, что я заметил, мы говорили о том, что, возможно, какие-то другие игроки, относящиеся к отрасли Интернета вещей, в этой экосистеме могут быть другие игроки, возможно, они... что им нужно делать для того, чтобы повысить безопасность, но я не понял, какая роль в этом отводится пользователю. Возможно, это не так просто, но что мы ожидаем от пользователей? На какой уровень информированности мы рассчитываем с их стороны, со стороны потребителей этих новых технологий? Иногда эти технологии затрагивают их даже в том случае, если они не являются непосредственными потребителями, я имею в виду, когда мы говорим об Интернете вещей и всех этих устройствах для умных домов.

Когда... кажется, Кристиан говорил о том, как мы должны помочь в том, что касается разумного использования, — это я, наверное, своими словами пересказываю — разумного использования DNS и оптимальных практических методик. Мне хотелось бы знать,

из моего собственного опыта в ICANN, например, когда мы вводили новые gTLD и интернационализированные домены, и еще у нас был этот опыт с универсальным принятием, может ли это быть как-то полезно или можно ли это... (неразборчиво)... какой-то подход, который можно было бы использовать для того, чтобы информировать людей о том, как это лучше использовать или как лучше работать с DNS в контексте Интернета вещей.

Так что мне хотелось бы знать, возможно, Кристиан, исходя из его опыта, а также из того, что он... он работал с доменом .NL, может ли он как-то развить этот опыт и сказать, есть ли какие-то области, которые пересекались бы в этом, и какие выводы мы можем извлечь из этого опыта.

И еще, наверное, один момент. Это... на мой взгляд, было полезно узнать подробнее о сетях 5G и о том, как они могут использоваться... в контексте Интернета вещей. И, возможно, узнать, как используется в этом... в этой области DNS. Но, возможно, если Лизе сможет как-то больше развить эту тему в том смысле, есть ли какая-то область политик, о которой нам нужно знать, когда речь идет о технологиях 5G.

И это все. Это все, что я хотел сказать.

Спасибо.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Рафик. Как я уже сказала, давайте сначала пройдемся по нашим рецензентам, а на вопросы можно будет ответить позже.

Кей Си, прошу вас.

КЕЙ СИ КЛАФФИ: Приветствую. Да, это были замечательные выступления. Я очень ценю ту работу, которая за ними стоит, и меня особенно заинтересовала работа над этим проектом SPIN, которым занимается лаборатория SIDN.

Мне интересно, кому что известно о том, насколько такого рода деятельность поддерживается правительствами. Мне известно, что в США в этой области уже много лет работает Национальный институт стандартов и технологий (NIST), я думаю, они видят, так сказать, прибытие поезда и хотят помочь отрасли в решении каких-то из этих проблем. Я вижу, что это движение к Интернету вещей вынуждает... или еще вынудит, наверное, мы пока еще не видели какой-то конфронтации, связанной с неспособностью решить многие фундаментальные проблемы с безопасностью, присущие архитектуре Интернета. Мы немало времени и сил потратили на разработку таких технологий, как DNSSEC и BGPSEC, когда организации, определяющие стандарты, пытались создать какие-то усовершенствования протокола, которые помогли бы решить какие-то конкретные проблемы безопасности, но для этого потребовалось бы их развертывание в глобальных масштабах, чего, к сожалению, не произошло.

В качестве альтернативных подходов предпринимались попытки предложить какие-то методики работы, к примеру, в пространстве протокола BGP это была концепция MANRS, то есть согласованные нормы обеспечения защищенности маршрутизации. В мире интернет-провайдеров это, по сути, такой кодекс поведения, что если сделать ряд каких-то вещей, это поможет сократить поверхность атаки, когда речь идет о встроенных уязвимостях в безопасности маршрутизации, которые нам не удалось преодолеть. Это технические средства.

Мне хотелось бы знать, не могли ли бы наши эксперты рассказать немного подробнее о том, считают ли они, что что-то в этом роде может быть полезным в пространстве Интернета вещей, поскольку в пространстве Интернета вещей нет возможности создать какой-то отдельный технический уровень, как мы пытались это сделать для протоколов маршрутизации и разрешения имен, поскольку протоколов Интернета вещей так много, что они, так сказать, функционально несовместимы между собой. То есть мне интересно, что вы думаете о чем-то таком же в этой сфере.

Это все, что я хотела сказать. Вы проделали замечательную работу.

Я опубликую какие-то URL-адреса в чате по работе NIST.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Кей Си.

Итак, эксперты, кто хочет начать?

ЭЛИОТ ЛИР: Это Элиот.

АЛЕХАНДРА РЕЙНОСО: Прошу вас.

ЭЛИОТ ЛИР: Прежде всего, все рецензенты отметили очень важные моменты, и спасибо вам за... за интересный разговор в чате. Это на самом деле очень увлекательная дискуссия.

Кей Си совершенно права в том, что институт NIST действительно тратит много времени и усилий на решение проблем с безопасностью Интернета вещей, а это очень много очень разных проблем. То есть, к примеру, есть такой документ NIST TR8228, в котором речь идет о соображениях, применимых к управлению Интернетом вещей, практике обеспечения кибербезопасности и сопутствующих этому рисках. Есть также проект рекомендаций SP1800-15, посвященный работе с атаками типа «отказ в обслуживании» в контексте Интернета вещей, в котором особое внимание уделяется описанию практики использования у разных производителей.

Еще один момент, а затем я передам слово другим, это то, что Интернет вещей — это не... это нечто очень туманное. В разных секторах бизнеса он работает по-разному. Мы уделяем очень много внимания потребительскому рынку, но есть еще и промышленное применение, есть умные города, есть сфера

здравоохранения. И важно понимать, что во многих из этих секторов уже очень строгое регулирование.

Просто один пример: управление по контролю за продуктами и медикаментами США регулирует использование любого терапевтического медицинского оборудования, независимо от того, подключается ли оно к Интернету, на него все равно распространяется регулирование и там очень много требований в том, что касается безопасности такого оборудования. И то же самое будет справедливо для другой критически важной инфраструктуры. Интернет вещей приходит, знаете ли, и в ядерную промышленность. Разумеется, это высокорегулируемый сектор.

Вопрос в том, какого рода регулирование или практика работы требуется в самых разных других областях, в которых мы наблюдаем новые способы использования Интернета вещей или которые, возможно, более надежно регулируются. Даже на потребительском рынке есть свое регулируемое пространство, и там больше вероятность того, что это регулируется.

Спасибо.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Элиот.

ЛИЗЕ ФУР: Я буду рада выступить следующей, если хотите.

АЛЕХАНДРА РЕЙНОСО: Да, Лизе.

ЛИЗЕ ФУР: На вопрос Филиппа о том, как лучше связываться с разными действующими лицами на рынке, я думаю, что сотрудничество или отчет SSAC — это очень хороший пример того, каким образом мы как операторы связи можем использовать эти возможности для того, чтобы связываться с нашими клиентами и партнерами, а также правительствами и другими действующими лицами для обсуждения оптимальной практики работы и способов обеспечения безопасности. Так что я считаю, что диалог между ними, ICANN и SSAC, а в Европе у нас есть агентство ENISA и институт ETSI. По-моему, это важно. Так что такое перекрестное общение нужно вести. А что касается ассоциации ETNO, мы на самом деле уже ведем такое общение с представителями других секторов и пользуемся такими возможностями.

К тому, что говорил Рафик, есть ли какая-то политика в области DNS и 5G, — в настоящее время в Европе есть множество разных правил в том, что касается сетей 5G и безопасности. А еще у нас есть новый законодательный акт, касающийся безопасности, и он затрагивает также сети 5G, но не конкретно DNS, однако я считаю, что по мере развития сетей 5G все больше внимания на самом деле будет уделяться использованию DNS в Интернете вещей... в контексте безопасности.

И еще у нас есть то, что мы называем набором инструментов безопасности 5G, это главным образом касается оборудования,

но я считаю, что это очень важный нормативный акт, который на самом деле затронет и различные аспекты использования DNS.

К тому, что говорила Кей Си о неспособности преодолеть проблемы безопасности, — это правда. Это такая область, в которой постоянно происходит какое-то движение в том, что касается нашего подхода к безопасности, потому что технологии развиваются очень и очень быстро.

В Европе у нас есть ENISA — это орган Еврокомиссии, занимающийся вопросами безопасности. И они на самом деле... они сейчас сформировали группу заинтересованных сторон по вопросам безопасности, в нее входят все заинтересованные стороны, которые будут обсуждать проблемы стандартизации в том, что касается безопасности. И я абсолютно уверена в том, что в рамках этого обсуждения будут затрагиваться также и области, касающиеся DNS и Интернета вещей. Спасибо.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Лизе. Я предлагаю нам... да?

КРИСТИАН ХЕССЕЛЬМАН: Я хотел только ответить на то, что сказал Рафик о роли пользователей.

АЛЕХАНДРА РЕЙНОСО: Прошу вас, Кристиан.

КРИСТИАН ХЕССЕЛЬМАН: Мы еще не затрагивали этот вопрос.

На мой взгляд, разумеется, пользователи — это важная составляющая этой формулы, потому что в конечном итоге ради этого-то мы все это и делаем. И я думаю, что нам нужно каким-то образом дать пользователям возможность лучше понять то, что происходит в сфере Интернета вещей, чтобы они больше отдавали себе отчет в том, что происходит, когда они сознательно взаимодействуют с устройствами ИВ, это может быть, например, какая-то визуализация или еще какое-нибудь представление того, как их личные данные передаются удаленным службам в Интернете. И это может на самом деле вызвать дискуссию или, если угодно, спрос со стороны потребителей на такого рода решения в области безопасности, в которых свою роль может сыграть и система DNS.

Кроме того, я считаю, что... с точки зрения гражданина, так сказать, это ведь тоже конечные пользователи, я считаю, что свою роль в этом должны сыграть и правительства, и другие регулирующие органы. И я вижу, что это уже происходит. То есть в Нидерландах, например, местный регулятор играет в этой сфере очень активную роль. Как NIST в США, например. И мы также наблюдаем различную деятельность в том, что... что касается европейской директивы по радиооборудованию, о которой я уже говорил. Так что я считаю, что в конечном итоге это тоже сведется к политике, когда представители государственных структур и регулирующих органов, возможно, таких как ICANN, по сути, установят некий стандарт обеспечения

минимального уровня кибербезопасности, который необходимо будет соблюдать в устройствах Интернета вещей.

Спасибо.

АЛЕХАНДРА РЕЙНОСО: Большое вам спасибо, Кристиан, а также всем остальным.

Сейчас мы пройдемся по вопросам, которые нам прислали в разделе вопросов и ответов конференции. Еще раз вам напомню, что задавать вопросы следует через панель вопросов и ответов. Вопросы из чата зачитываться не будут.

Итак, мы готовы к ответам на вопросы? Рия?

РИЯ ОТАНЕС: Здравствуйте, Алехандра. У нас вопрос от Энджи Матлапенг (Angie Matlapeng): Было ли предложено какое-то решение проблемам, которые возникают с памятью на миниатюрных — например, носимых, — устройствах ИВ при попытках использовать для защиты этих устройств DNSSEC и шифрование?

ЭЛИОТ ЛИР: Может, я попробую ответить на это?

АЛЕХАНДРА РЕЙНОСО: Прошу вас.

ЭЛИОТ ЛИР: Энджи, большое вам спасибо за этот вопрос. Интернет вещей действительно сталкивается с некоторыми проблемами, касающимися шифрования и использования памяти. Первая из них — это то, что, конечно же, когда речь идет, в частности, о потребительских устройствах и прочем миниатюрном оборудовании, память там на вес золота. Я буквально спорил с разработчиками ИВ практически за каждый байт.

А если вы посмотрите на то, какой стек там используется, они пользуются специализированными криптографическими стеками, например OV SSL, — это хороший пример высокооптимизированного стека шифрования. Если вы посмотрите на размер SSL, там может быть больше мегабайта размер. А в OV SSL, просто чтобы вы себе представили разницу, в аналогичном случае от 14 килобайт.

Но Интернет вещей сталкивается еще с одной проблемой, когда речь идет о перспективе, а именно с тем, что такие устройства, как кто-то уже сказал — Кристиан уже говорил об этом в своем выступлении, — у них очень большой срок службы.

А шифрование... в области криптографической защиты уже много лет все постоянно меняется. То, что казалось нам приемлемой защитой пять лет назад, или десять лет назад, сегодня уже очень уязвимо перед атаками. А если представить себе такие устройства, как буровые вышки или нефтяные платформы, когда вы погружаете устройство в грунт на 40 лет, представьте себе... не представьте. Вспомните, что у нас было 40 назад

в плане технологий. А теперь представьте себе, каково это — пытаться обновить такое устройство, чтобы оно использовало современные технологии. Ему 40 лет, представьте себе задачу модернизации устройства, которому 40 лет. Это сложная задача для Интернета вещей. И не похоже, чтобы у нее были простые решения.

Кто-то, кажется, это был Дэн Гир (Dan Gear) из Массачусетского технологического института, опубликовал замечательный доклад, в котором речь шла о таком решении, там предлагалось оснащать устройства ИВ таким, по сути, выключателем, который просто отключал бы их от сети. Разумеется, могут быть ситуации, в которых это возможны, и другие, в которых нет. Но это пища для размышлений. Это был замечательный документ. Спасибо.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Элиот. Кажется, у нас есть еще один вопрос.

РИЯ ОТАНЕС: Да. Следующий вопрос: считаете ли вы... от Анупам Агравак (Anupam Agrawak): Считаете ли вы, что существующая система идентификаторов сможет удовлетворить требованиям к безопасности в случае Интернета вещей?

ЭЛИОТ ЛИР: Я думаю, все молчат, потому что на этот вопрос очень трудно ответить.

Кристиан, прошу вас.

КРИСТИАН ХЕССЕЛЬМАН: Мы говорили о... на самом деле я считаю, что тут есть два момента. Один — это то, что система идентификаторов, которая в данном случае... в контексте того, о чем мы говорим, идентификаторами служат доменные имена. То есть их можно защищать, чтобы повысить конфиденциальность пользователей. Мы говорили об этом ранее в ходе этой дискуссии.

Но, разумеется, есть и другое измерение: какого рода информацию ваши устройства передают в удаленные службы? То есть это может касаться собственно содержания, а может касаться и особенностей трафика, потому что были исследования, которые показывали, как можно угадать, каким устройством вы пользуетесь у себя дома. Просто проанализировав особенности трафика, не учитывая при этом его содержание.

Так что я считаю, что на эту проблему следует смотреть под разными углами, если речь идет о том, чтобы защитить конфиденциальность пользователей. То есть здесь может иметься в виду защита сообщений, которые используются при работе с системой идентификаторов, в данном случае это DNS. Однако есть еще и собственно трафик, который передается, который вы отправляете в удаленные службы или который вы от них получаете, и речь может идти о защите этой информации, как посредством шифрования, так и посредством, возможно, даже обфускации, то есть попыток скрыть информацию, которая позволяла бы определить, какого рода устройство взаимодействует с удаленной службой.

Я согласен с Элиотом, что это сложный вопрос.

[смеется]

АЛЕХАНДРА РЕЙНОСО: Большое вам спасибо, Элиот и Кристиан. Элиот, я не знаю, возможно, вы хотите как-то это прокомментировать?

ЭЛИОТ ЛИР: Я хотел попробовать ответить на вопрос Найджела. Он спрашивал о проблемах, связанных с использованием протокола IP в качестве механизма доставки в сетях 5G в контексте Интернета вещей и стандартов.

Я считаю, что определенные проблемы для 5G существуют. Главная из них — как ограничить поверхность угроз для этих устройств? Каким образом провайдер... какова роль провайдера в сокращении площади угроз? И как... какое взаимодействие имеет место между контрольной точкой сети — которая, по сути, представляет собой фильтр пакетов, — и системой DNS в мире облачных вычислений?

И те же проблемы, о которых я говорил в контексте домашних систем, они же стоят и перед сообществом 5G. И мы уже начали обсуждать эти проблемы, но пока мы все еще в самом начале пути.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Элиот.

Мы зачитаем еще один, последний вопрос, потому что, к сожалению, у нас заканчивается время.

Прошу вас, Рия.

РИЯ ОТАНЕС: У нас вопрос от участника по имени Суада Хаджович (Suada Hadzovic). Если у нас есть облачные провайдеры служб Интернета вещей, как это соотносится с режимами туманных вычислений, или краевых, периферийных вычислений? NIST определяет туманные узлы как физические компоненты, такие как шлюзы т. п.

ЭЛИОТ ЛИР: Хорошо. Я попробую ответить и на этот вопрос тоже.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Элиот.

ЭЛИОТ ЛИР: Спасибо. Я уже пытался однажды на него ответить. Итак, для устройств Интернета вещей используются различные модели вычислений.

И, как я уже сказал в одном из ответов, стоимость товаров и услуг на фактическом узле, если это возможно... производители стараются держать стоимость на очень низком уровне.

Но иногда нужно... они делают следующее — они переносят значительную часть вычислительной мощности в облако, потому что его легко масштабировать. Если облако... если производителю или оператору службы нужно больше мощности, ее можно добавлять по мере роста потребностей. Облако для этого замечательно подходит.

Однако есть область, в которой облачным системам присущи определенные ограничения, — это задержки, и чтобы преодолеть их, нужно использовать локальные вычислительные мощности. И в этом заключается идея туманных вычислений.

Я бы сказал, что эта область требует дополнительного изучения. В потребительском секторе вы этого не увидите, однако туманные вычисления часто используются для промышленного применения, когда локальные контроллеры позволяют расширить возможности в том, чтобы обрабатывать данные на месте и координировать обмен данными между устройствами Интернета вещей.

Это уже широко используется в сфере промышленного применения, но в этой области еще осталось много возможностей для изучения.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Элиот.

На этом я буквально в нескольких предложениях подведу итог сказанному. Для нас очень важно поддерживать дискуссию в том,

что касается возможностей, рисков и проблем, проистекающих из взаимодействия между системой DNS и Интернетом вещей.

Важно понимать, что такое взаимодействие бывает пассивным. Это значит, что пользователь не знает, что происходит с его устройствами. Это то, над чем предстоит поработать.

Конфиденциальность — это проблема, и безопасность —это проблема. В этом смысле есть определенные сложности. Сообщество ICANN может сосредоточить свои усилия на том, чтобы несколько расширить свое понимание этих рисков и проблем, а также того, каким образом различные организации сообщества и консультативные комитеты могут внести свой вклад в усовершенствование взаимодействия между Интернетом вещей и DNS.

Я хочу поблагодарить всех наших экспертов и рецензентов за их совместную работу и за уделенное ими время, а также персонал ICANN, который обеспечивал поддержку этого пленарного заседания. Вы все отлично поработали.

Это пленарное заседание подошло к концу. Большое спасибо за участие. До встречи в следующий раз.

До свидания.

[КОНЕЦ СТЕНОГРАММЫ]