ICANN71 | Виртуальный форум по формированию политики — презентации NextGen, день 1
Вторник, 14 июня 2021 г. – с 14:30 до 16:00 CEST

ДЕБОРА ЭСКАЛЕРА (DEBORAH ESCALERA):

Хочу поблагодарить всех за то, что присоединились к нам сегодня. Доброе утро, добрый день, добрый вечер! Здравствуйте и приветствую вас на презентации ICANN71. Меня зовут Дебора Эскалера, я работаю в отделе обеспечения ответственности перед общественностью и руковожу программой NextGen@ICANN. На этом заседании я буду координатором удаленного участия. Обратите внимание, что заседание записывается, и мы соблюдаем Стандарты ожидаемого поведения ICANN. Во время заседания будут зачитываться только те вопросы и комментарии, которые отправлены с помощью функции вебинара Q&A. Я буду зачитывать вопросы вслух во время, указанное председателем или модератором этого заседания.

Выступления будут переводиться на много языков. Нажмите «Устный перевод ICANN» в Zoom и выберите язык для прослушивания во время этого заседания.

Если вы захотите выступить, поднимите руку в Zoom, и после того как координаторы конференции назовут ваше имя, наша группа технической поддержки даст вам возможность включить микрофон. Прежде чем выступить, выберите в меню перевода язык, на котором будете говорить. Назовите для протокола свое имя и язык выступления, если это не английский.

Когда будете говорить, отключите звук и уведомления на всех остальных устройствах. Пожалуйста, говорите четко и с нормальной скоростью, чтобы обеспечить точный перевод. Все участники могут оставлять в чате комментарии. Для этого выберите пункт «Ответить всем участникам группы и присутствующим» в раскрывающемся меню чата. После этого все смогут увидеть ваш комментарий.

Обратите также внимание, что закрытые чаты возможны только для участников публичной дискуссии в формате вебинара Zoom. Любое сообщение, отправленное участником или обычным присутствующим другому обычному участнику, увидят организаторы, соорганизаторы и докладчики.

Хочу выразить особую благодарность моим менторам, помогавшим мне подготовить студентов в течение нескольких недель перед ICANN71. Они проделали огромную работу. Чери Стаббс (Cherie Stubbs), Арис Игнасио (Aris Ignacio) и Дессален Иегуала (Dessalegn Yehuala). Большое спасибо. Они мне очень помогли подготовить студентов к ICANN71 — провели их через процесс и подготовили к сегодняшнему дню.

Нашим первым докладчиком будет Даниил Голубев. Надеюсь, он в комнате и готов говорить. Фернанда, моя коллега, сегодня будет помогать мне со слайдами. Фернанда, спасибо за помощь сегодня. Даниил, вы в комнате?

ДАНИИЛ ГОЛУБЕВ (DANIIL GOLUBEV):

Да, я готов к презентации. Добрый день! Всех приветствую!

ДЕБОРА ЭСКАЛЕРА: Хорошо. Хочу еще раз попросить всех докладчиков говорить внятно и с разумной скоростью, чтобы наши переводчики смогли перевести все, что вы скажете. Также напоминаю, что вы должны говорить Фернанде: «Следующий слайд, пожалуйста». Большое спасибо, Даниил, вы можете начинать.

ДАНИИЛ ГОЛУБЕВ: Хорошо. Уважаемые коллеги, всем добрый день. Я хочу поговорить об очень специфической проблеме, а именно о точке зрения Российской ассоциации цифровых технологий в отношении регулирования интернета и общего состояния свободы интернета в России. Этот вопрос, разумеется, довольно узкий, но его можно экстраполировать с России на другие страны. Следующий слайд, пожалуйста.

В России есть ассоциации, деятельность которых направлена на развитие интернет-индустрии — так называемые интернет-ассоциации. Их [неразборчиво] существования и характер их [неразборчиво] различны. Основным критерием выбора ассоциаций для этой презентации было их позиционирование себя как организаций, независимых от государства. Однако мой анализ их работы и функционирования показывает, что это может не соответствовать истине, и в этой презентации я попытался определить позиции ассоциаций в отношении регулирования интернета, выраженные различным образом.

В этой презентации я рассматриваю следующие ассоциации и организации: Ассоциация защиты авторских прав в интернете, Медиа-коммуникационный союз, Региональный общественный центр интернет-технологий, Российская ассоциация электронных коммуникаций и Институт развития интернета. В

России, разумеется, ассоциаций намного больше, но я выбрал самые крупные и влиятельные в российском сегменте интернета. Следующий слайд, пожалуйста.

Хочу немного рассказать о состоянии свободы интернета в России. Российские органы власти стремятся как можно более жестко регулировать российский сегмент интернета, и я хочу рассказать о нескольких примерах взаимоотношений между интернетом и правительством России и том, как оно его регулирует.

В России есть орган власти, называемый Роскомнадзор, который цензурирует российский сегмент интернета и блокирует множество сайтов, которые, по его мнению, нарушают закон. Этот исполнительный орган власти блокирует множество источников информации в России.

Также граждане России могут понести ответственность за оскорбительные комментарии в интернете в адрес органов власти. В России не так давно прошли протесты и демонстрации, и наблюдались отключения мобильных сетей не без участия правительства.

Предпринимаются попытки изолировать российский сегмент интернета от остального мира и создать так называемый суверенный интернет или Рунет, как мы его называем в России. Международные компании, работающие в ИТ-индустрии, обязаны хранить свои данные о российских пользователях на территории России, чтобы российские органы власти могли получать доступ к данным российских пользователей. Следующий слайд, пожалуйста.

Первой ассоциацией, о которой я хочу рассказать, является ассоциация защиты авторских прав в интернете — АЗАПИ. Это некоммерческая партнерская организация, деятельность которой направлена на борьбу с незаконным размещением книжной и аудиопродукции в интернете. Ее деятельность в основном ассоциируется с нарушением авторских прав. АЗАПИ участвует в обсуждении проектов законов, связанных с защитой авторских прав в российском сегменте интернета. Среди ее клиентов крупные российские издательства, стремящиеся защищать свои авторские права. К сожалению, эта ассоциация не предлагает очень эффективных мер для удовлетворения этих потребностей. Следующий слайд, пожалуйста.

Как АЗАПИ взаимодействует с правительством России? В 2015 году АЗАПИ подала иск в суд города Москвы с запросом заблокировать торрент-трекер RuTracker, хранящий объекты авторского права клиентов АЗАПИ. Иск не просто был удовлетворен, но одновременно был подан запрос на блокировку всего сайта, всего торрент-трекера, что, к сожалению, нехорошо для состояния интернета.

В 2016 году АЗАПИ подала в суд города Москвы иск с требованием обязать поисковую систему Яндекс, вторую по популярности поисковую систему в России после Google, удалить ссылки на книги, связанные с RuTracker, из результатов поиска.

В 2019 году АЗАПИ подала в суд города Москвы серию исков против ресурса Archive.org, который хранил в кэше цифровые копии аудиокниг писателей Дмитрия Глуховского и Дарьи Донцовой, которые также были клиентами АЗАПИ.

В 2020 году АЗАПИ подала иск в Европейскую комиссию относительно признания ответственности Google за отказ удалить из Google Play приложения, способствующие «массовому нарушению авторских прав» на электронные книги. Вот эти сайты — Ok.ru, Mail.ru, Telegram, YouTube и WattPad. Следующий слайд, пожалуйста.

Дальше у нас Медиа-коммуникационный союз или МКС. Он был создан в 2014 году крупнейшими игроками в медиа и телекоммуникациях. Это некоммерческое партнерство российских медиакомпаний и телекоммуникационных операторов, выступающих посредниками между телекоммуникационными и медиакомпаниями. Следующий слайд, пожалуйста.

В разные годы Медиа-коммуникационный союз предлагал правительству России несколько законопроектов, в основном в период руководства Павла Степанова, который был президентом МКС с 2016 по 2018 год. МКС предложил такой [неразборчиво] как внесудебная блокировка зеркал пиратских сайтов, блокирование торрентов на уровне протокола пользовательских дейтаграм DNS, регулирование приложений для обмена сообщениями и работы онлайн-кинотеатров. Следующий слайд, пожалуйста.

Еще одна ассоциация — Региональный общественный центр интернет-технологий или РОЦИТ. Он был основан в 1996 году. Члены правления РОЦИТ включают представителей правительственных агентств и коммерческих компаний. Эта организация финансируется Фондом президентских грантов. То есть она косвенно финансируется правительством, даже несмотря на то, что это неправительственная ассоциация. Цель ее работы заключается в создании дружелюбной интернет-среды и популяризации интернет-технологий. Она позиционируется как платформа взаимодействия между пользователями, компаниями и государством, а также как орган, занимающийся решением проблем, связанных с ИТ-индустрией. Следующий слайд, пожалуйста.

РОЦИТ связан с реакцией российских органов власти на протесты. В 2021 году в России произошли массовые антиправительственные протесты, масштабно подавленные правительством физическими и цифровыми средствами. Реакция РОЦИТ на распространение через соцсети контента, который, по мнению этой организации, популяризирует экстремизм:

«Эксперты РОЦИТ отмечают резкое возрастание количества материалов, направленных на нарушение общественной безопасности в интернете». В этом сообщении они критикуют контент, который просто информирует людей о протестах. И они называют материалы о протестах экстремистской и даже террористической деятельностью.

РОЦИТ обратился к соцсетям с требованием прекратить распространение такого контента, связанного с протестной деятельностью. Позиция РОЦИТ совпадает с позицией правительства. Следующий слайд, пожалуйста.

Есть еще одна ассоциация — Российская ассоциация электронных коммуникаций или РАЭК. Она была основана в 2006 году. Она включена в перечень получателей государственной помощи в сфере электронных медиа, то есть также финансируется правительством. Среди основных членов РАЭК крупнейшие в России ИТ-компании — Mail.ru Group, Лаборатория Касперского, ВКонтакте, Ростелеком.

Также она включает государственные компании, такие как информационное агентство Russia Today и новостное агентство ТАСС. Это некоммерческая организация, представляющая интересы рынка электронных коммуникаций России, деятельность которой направлена на консолидацию мнений отраслевых лидеров и взаимодействие с правительственными агентствами. Следующий слайд, пожалуйста.

Позиция относительно регулирования РАЭК интернета выражается Премией Рунета. Эта Премия вручается РАЭК за достижения в российском сегменте интернета, а с 2011 года она вручается в номинации за регулирование российского сегмента интернета, такой как безопасный Рунет (интернет без экстремизма), социально значимым проектам, направленным, в частности, на защиту детей и укрепление цифрового «иммунитета» Рунета.

В большинстве случаев, в этих категориях, единственными победителями являются государственные компании, деятельность которых направлена на цензурирование российского сегмента интернета. В категориях, связанных с информационным контентом интернета, в большинстве случаев, предпочтение отдается государственным ресурсам. Следующий слайд, пожалуйста.

Последней ассоциацией, о которой я хотел бы рассказать, является Институт развития интернета или ИРИ. Он был учрежден в 2015 году при поддержке администрации президента. Но, все равно, позиционировался как неправительственная ассоциация. Это независимая некоммерческая организация, основная деятельность которой нацелена на производство социально значимого контента в интернете и разработку проектов отраслевых законов. Она служит посредником между игроками цифровой отрасли и государственными агентствами и проводит тендеры на производство видеопродукции в сфере социальной рекламы и патриотического контента. Это своего рода рынок контента в интернете, в российском сегменте интернета, на социальную тематику. Следующий слайд, пожалуйста.

Как ИРИ участвовал в регулировании цифровой отрасли в разные годы? Они предложили перечень российского ПО для предустановки на ноутбуки и смартфоны. Они предложили факультативную программу для киберспорта. Они предложили разработать меморандум о социальной рекламе. Они предложили создание безопасной цифровой среды для младшего поколения. Они предложили создать программы обучения по цифровым технологиям. А также они предложили

регулировать анонимайзеров в США, включая VPN. Следующий слайд, пожалуйста.

Как эти ассоциации связаны? Не существует органа, координирующего работу в отношении проблем регулирования интернета. Однако их члены представлены друг в друге. Члены МКС присутствуют и в РОЦИТ, а правительство России является членом или оказывает какое-то давление на каждую из упомянутых ассоциаций.

Как это связано с ICANN? РОЦИТ и ИРИ числятся среди основателей российского центра координирования доменов верхнего уровня, обеспечивающих функционирование российских доменов верхнего уровня, таких как .ru и .rf. Это значит, что через такие негосударственные ассоциации, учитывая, что они связаны с правительством, правительство может влиять на политику доменов верхнего уровня и работу каждой ассоциации. Следующий слайд, пожалуйста.

Подытожу: 1. Многие интернет-ассоциации, даже зарегистрированные как некоммерческие и негосударственные, связаны с государственными структурами в России, финансируются через государственный бюджет и регулируются правительственными указами, а члены правительства присутствуют в ассоциациях, что влияет на выражение мнений в них.

2. Решения ассоциаций принимаются большинством голосов членов, среди которых представлены органы власти России. В большинстве случаев они позитивны и способствуют регулированию интернета. В очень редких случаях они умеренно критичны к определенным вопросам.

3. Сами ассоциации получают выгоды от регулирования, поскольку занимаются выполнением правительственных указов по исполнению принятых законов. Они лоббируют свои интересы при обсуждении или представлении проектов законов и пытаются монополизировать определенные коммерческие сферы, концентрируя определенные аспекты вокруг одной ассоциации и ослабляя конкурентов.

Наконец, хочу сказать, что российское правительство пытается максимально возможным образом регулировать интернет, и ассоциации — один из способов такого регулирования, потому что, даже если на бумаге такие ассоциации не связаны с правительством, они так или иначе им регулируются. Спасибо за внимание.

ДЕБОРА ЭСКАЛЕРА: Прекрасно. Спасибо, Даниил. Есть какие-либо вопросы к Даниилу? Вы можете поднять руку или задать вопрос в чате.

ДАНИИЛ ГОЛУБЕВ: Есть вопрос от Пабло.

ДЕБОРА ЭСКАЛЕРА: Пабло, включите микрофон и задайте вопрос.

ПАБЛО БУРДЯК (PABLO BURDIAK): Да. Приветствую всех. Прежде всего, хочу поблагодарить Даниила за такую отличную и информативную презентацию. Меня очень интересует этот вопрос, поскольку мои исследования частично касаются и России. Хочу спросить, есть ли в России ассоциации, не связанные с правительством ни прямо ни косвенно, то есть независимые?

ДАНИИЛ ГОЛУБЕВ: Спасибо за отличный вопрос, Пабло. К сожалению, у меня было мало времени — всего 10 минут. Да, есть абсолютно независимые ассоциации, но в большинстве случаев им не разрешают регистрироваться законным образом, потому что для этого нужно полностью выполнить законы и нормы России. Приходится искать компромисс и, в большинстве случаев, это не получается.

Есть ассоциация Роскомсвобода. Она занимается вопросами свободы интернета и является уполномоченным отделением ICANN в России в определенных вопросах. Ее работа нацелена на обеспечение максимальной свободы интернета в России. Но, к сожалению, в большинстве случаев им не разрешают работать на официальном уровне.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо. У нас есть вопрос от Риккардо Нанни. Риккардо.

РИККАРДО НАННИ (RICCARDO NANNI):

Спасибо вам, Даниил, за очень интересную презентацию и подробную информацию. Мы периодически слышим о Рунете, но нам сложно понять, что за этим кроется.

В последнее время говорили о возможности учредить российскую систему доменных имен в России. Это просто обсуждение возможностей или будут какие-то конкретные действия? У вас есть мнение по этому поводу? Спасибо.

ДАНИИЛ ГОЛУБЕВ: Спасибо за вопрос, Риккардо. Да, предпринимаются попытки учредить так называемый суверенный интернет, Рунет, с российской системой доменных имен. Об этом говорят, мне кажется, с 2010 года. Российское правительство и ИТ-специалисты, работающие на правительство, пытались учредить так называемый независимый интернет для России.

Однако их квалификация недостаточна. В 2017 году Россия пыталась заблокировать Телеграм. Не получилось. Телеграм все еще работает в России. В этом году они пытались заблокировать Твиттер. Это тоже не получилось и сейчас они говорят о блокировке YouTube, что достаточно… Не думаю, что это получится, потому что квалификация ИТ-специалистов, работающих на правительство, просто недостаточна.

Да, идут разговоры о том, чтобы сделать интернет более суверенным, но я не думаю, что в текущей ситуации распространения интернета в России там можно сделать что-то такое, как в Китае. Мировое сообщество просто слишком интегрировано в российский сегмент интернета и я не думаю, что такое можно будет сделать в крупном масштабе.

ДЕБОРА ЭСКАЛЕРА: Большое спасибо за отличную презентацию, Даниил. Хорошо, перейдем к нашему следующему докладчику, Веронике Сломинска.

ВЕРОНИКА СЛОМИНСКА (WERONIKA SLOMINSKA): Здравствуйте!

ДЕБОРА ЭСКАЛЕРА: Напоминаю: у вас 10 минут, если вы превысите этот лимит, я дам вам предупреждение. Также прошу вас говорить четко и медленно. Спасибо.

ВЕРОНИКА СЛОМИНСКА: Хорошо. Спасибо. Приветствую всех. Благодарю вас Даниил за очень интересную презентацию. Меня зовут Вероника. Я изучаю управление международной общественной деятельностью и сегодня хочу поговорить о кибербезопасности и проблемах, с которыми сталкиваются в этой связи те, кто разрабатывает политики, а также о необходимости повышения осведомленности об этой проблеме. Следующий слайд, пожалуйста.

Спасибо. Кибербезопасность становится все более масштабной и часто возникающей проблемой по всему миру. Постоянно появляются новые виды киберугроз, а кибератаки могут оказывать очень сильное влияние на всех людей и организации, что означает, что этот вопрос требует подхода от общего к частному.

Кибербезопасность — многогранная проблема, для решения которой требуется сотрудничество между людьми, занимающимися техническими аспектами и регулированием. Именно об этом я хочу рассказать сегодня.

В мире интернета вещей все больше и больше физических предметов имеют свой IP-адрес для подключения к интернету и связи, что означает, что общество все больше зависит от киберпространства. Однако, даже несмотря на то, что киберпространство играет такую важную роль, правительства, как видится, делают недостаточно для обеспечения его безопасности, и киберпространство не получает того внимания, которого требует. Следующий слайд, пожалуйста.

Причиной этого является то, что разработка политик в поле кибербезопасности сталкивается с множеством парадоксов, первым из которых является то, что правительства желают обеспечить кибербезопасность, но, с другой стороны, хотят получать данные граждан для надзора. С одной стороны, правительства хотят защитить своих граждан, но, с другой, не хотят, чтобы они использовали шифрование и другие меры обеспечения кибербезопасности. Так как они могут также использоваться преступниками и террористами.

Другой парадокс заключается в том, что кибербезопасность является глобальным явлением и не может быть обеспечена в пределах национальных границ, а требует транснационального подхода. Некоторые правительства не доверяют другим и не желают сотрудничать. Они даже могут взламывать системы других стран. Это все усложняет.

Другой очень важный парадокс заключается в том, что нет определенной суммы, которую правительство должно тратить на кибербезопасность, а это означает, что слишком низкие затраты не обеспечат достаточной защиты, а слишком высокие могут привести к ощущению того, что происходит что-то слишком плохое, и посеять панику. Поэтому баланс очень важен. Следующий слайд, пожалуйста.

Мы определили четыре основные причины того, почему разработка политик в области кибербезопасности очень проблемная. Во-первых, ограниченная видимость проблемы. Поскольку влияние нарушения кибербезопасности часто нельзя увидеть на физическом уровне и эту проблему не просто объяснить обществу, общество не чувствует реальной величины проблемы. Поэтому сложно разрабатывать политики для создания чего-то нового для решения чего-то невидимого.

Вторая проблема связана со сложностью социальных технологий обеспечения кибербезопасности. Хотя ИТ-инфраструктура и политики важны для обеспечения кибербезопасности, основную задачу выполняют люди, занимающиеся управлением системами и внедрением политик, но у многих людей и организаций недостаточно осведомленности и ресурсов для принятия мер.

Третья проблема заключена в соревновательной природе кибербезопасности. Хакеры зачастую действуют анонимно, поэтому непонятно, кто является врагом. Четвертая проблема состоит в сложности понимания степени влиянии. Сложно заранее оценить риски кибербезопасности и еще сложнее оценить влияние новых политик кибербезопасности, что усложняет поиск инвестиций. Следующий слайд, пожалуйста.

Как видим, существует огромная неясность и недостаточная осведомленность в отношении кибербезопасности, что приводит к возникновению проблем для тех, кто разрабатывает политики. Что же можно сделать для их решения? Следующий слайд, пожалуйста.

Исследователи подготовили информационную концепцию для простого и убедительного информирования о сложных проблемах. Поскольку разработчиков политик и специалистов часто критикуют за неспособность эффективно информировать общество из-за сложности специфики кибербезопасности, их послания нужно упростить до основной сути кибербезопасности и ее важности для людей. Следующий слайд, пожалуйста.

Исследователи предлагают следующую стратегию информирования для повышения осведомленности общества о вопросах кибербезопасности. Она будет состоять из шести этапов или правил. 1 — реалистичность, без усугубления значимости кибербезопасности и рисков, так как это усугубит саму проблему.

2 — четко обозначить, кто является преступниками, с кем мы сражаемся, кто может быть нашими врагами и со стороны кого можно ожидать угроз.

3 — обозначить героев и продемонстрировать тех, кто, например, в стране защищает кибербезопасность, их возможности и успехи.

4 — продемонстрировать важность кибербезопасности для общества, чтобы связать необходимость ее повышения с экономическим ростом и национальным благосостоянием.

5 — персонализировать вопросы кибербезопаности и связать их с повседневной жизнью людей, чтобы продемонстрировать, как она может влиять на повседневную жизнь людей и каким образом.

6 и последнее правило — связать два других вопроса, связанных с кибербезопасностью, таких как политики.

На следующем слайде хочу поблагодарить всех вас. У меня все. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Вероника. Очень хорошая презентация. У нас есть вопросы к Веронике? Есть вопросы в чате или кто-то поднимал руку? Хорошо, большое спасибо. Если у вас возникнут вопросы к Веронике, пишите нам или ей на электронную почту. Мы можем дать ее адрес электронной почты или вы можете писать на engagement@icann.org.

Следующую презентацию проводит Антронос Мулугета. Это будет видеопрезентация. Мне никогда этого не приходилось делать раньше, для меня это впервые. Сейчас я включу демонстрацию экрана для всех. Надеюсь, все получится. Вы его видите?

АНТРОНОС МУЛУГЕТА (ANTRONOS MULUGETA):

Приветствую всех. Меня зовут Антронос [неразборчиво]. Если у вас есть какие-либо вопросы, предложения или комментарии об этой презентации, пишите мне на электронную почту [неразборчиво].

Если речь идет о теме, которую [неразборчиво], как мы можем помочь ICANN с искусственным интеллектом? Чтобы сделать [неразборчиво] более конкретным и применить его для защиты системы доменных имен. Давайте вспомним, когда эта система доменных имен была придумана. Она была придумана в 1980 году и не предусматривала защиты для обеспечения [неразборчиво] или данных.

На тот момент интернет не был так широко распространен, как сегодня, и они не беспокоились о безопасности или защите, поэтому защита не была предусмотрена. Сегодня же интернет растет [неразборчиво], и это позволяет хакерам отклонять пользователей от нужного пункта назначения в пункты назначения, выбранные хакерами.

Когда Инженерная проектная группа интернета впервые занялась этой проблемой, они пытались создать решение и придумали DNSSEC — расширение безопасности системы доменных имен, нацеленное на усиление аутентификации источника данных, целостности данных в системе доменных имен с помощью цифровой подписи на базе открытого криптографического ключа.

Позвольте сказать, что аутентификация источника данных [неразборчиво], целостность данных, под аутентификацией источника данных я имею в виду то, что система доменных

имен, прежде всего, не обеспечивает ее, то есть не предоставляет уверенности в том, что данные связаны с [неразборчиво]. И, когда мы говорим «прежде всего», это не о [неразборчиво] целостности данных, а о невозможности предоставления [неразборчиво], если данные в ответе системы доменных имен были изменены или заменены. Таким образом, прежде всего, эта система доменных имен не была так защищена, как мы видим. Однако после внедрения DNSSEC это расширение системы доменных имен обеспечивает уверенность в том, что аутентификация источника данных [неразборчиво] целостность данных, поэтому безопасность повышается.

Однако это расширение не работает автоматически. Оно должно быть включено оператором и владельцем системы доменных имен. Это значит, что каждый владелец доменного имени должен знать о таком расширении, чтобы сделать интернет более безопасным.

Существуют разные владельцы доменных имен, например, бизнесмены, [неразборчиво] примеры использования для пояснения сайта [неразборчиво] с доменным именем, коммерческого сайта, который он использует для продажи своей продукции. Этот человек, как я говорил, бизнесмен, и не очень много знает о технической части вопроса, то есть он не может активировать DNSSEC [неразборчиво] для обеспечения безопасности. Это означает, что хакеры могут использовать такую же страницу для привлечения его клиентов.

Моя идея заключается в том, что для защиты этих людей эту систему можно сделать автоматической. Думаю, что можно применить искусственный интеллект и сделать систему автоматической.

Думаю, что есть люди, не понимающие технических вопросов. Если говорить о том, что такое искусственный интеллект и машинное обучение, то искусственный интеллект — это большой подраздел информатики, связанный с созданием машин или систем, способных выполнять задачи, требующие человеческого мышления или умения рассуждать.

С точки зрения [неразборчиво] я хочу поговорить только о конкретной части, применимой к этой сфере, а именно о машинном обучении искусственного интеллекта. Машинное обучение является частью искусственного интеллекта и заключается в обучении машин выполнению этой задачи хотя бы отчасти — так называемого контролируемого обучения. Контролируемое обучение является частью машинного обучения, состоящего в том, чтобы пометить или определить данные для обучения машин.

Это, конечно, сложный технический вопрос, но хочу вкратце объяснить, как можно применять это машинное обучение или искусственный интеллект. Я думаю, что мы можем научить машины понимать, когда регистрируется новая система доменных имен, а затем автоматически включать DNSSEC для повышения безопасности системы доменных имен.

Моя идея заключается в том, чтобы создать машину, способную понимать, когда регистрируется новая система доменных имен, и автоматически включать DNSSEC без необходимости привлечения владельца доменного имени и оператора. Думаю, что это поможет повысить безопасность интернета.

Мое исследование, я не пришел к однозначному выводу, но продолжаю работать над этим, мое исследование посвящено тому, можно ли включать ее автоматически через машинное обучение. Я хотел бы знать, что другие делают в этой связи, в связи с безопасностью интернета, чтобы сделать его более безопасным. Различные эксперты в настоящее время работают над применением машинного обучения для обнаружения [неразборчиво].

Я знаю, что это немного сложно и более техничный алгоритм [неразборчиво], чем [неразборчиво], используемый им для регистрации и классификации [неразборчиво], и они используют дополнительную информацию и такие решения, как Python в качестве базы программирования.

Я понимаю, что этот сложный вопрос нельзя рассмотреть за выделенные мне минуты, поэтому это все, что я могу рассказать сегодня. Если у вас есть вопросы, свяжитесь со мной по электронной почте. Большое спасибо за [неразборчиво] и особая [неразборчиво] за предоставление возможности подготовить презентацию. Спасибо всем вам и отличного дня.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Мне показалось, что у переводчиков возникли сложности, поэтому этой части не будет в стенограмме. Кажется, что к Веронике были вопросы, которые я пропустила. У кого-то есть вопросы к Веронике, которые я пропустила? Не могли бы вы поднять свою руку? Кто-нибудь? Если нет, продолжаем.

Наш следующий докладчик Вероника Пикколо. Вероника, вы онлайн?

ВЕРОНИКА ПИККОЛО (VERONICA PICCOLO): Да, я здесь.

ДЕБОРА ЭСКАЛЕРА: Хорошо, Вероника. У вас 10 минут. Прошу говорить медленно и разборчиво. Давайте, Вероника. Спасибо.

ВЕРОНИКА ПИККОЛО: Спасибо. Приветствую всех. Хочу рассказать о разбирательствах в двух итальянских судах в 2019 и 2020 годах по вопросам защиты прав на интеллектуальную собственность и, в особенности, о том, как их решения могут повлиять на целостность интернета и критически важные свойства интернет-сети. Следующий слайд, пожалуйста.

Это повестка. Сначала кратко расскажу об интернет-сети, ситуации, к которой приведут постановления суда, и их влиянии на критически важные свойства интернета, интернет-сеть, а затем расскажу о своем предложении. Следующий слайд, пожалуйста.

Немного об истории вопроса. В 2019 году итальянская медиакомпания обратилась за средством правовой защиты против Cloudflare. Cloudflare — поставщик услуг сети передачи данных, смягчения последствий DDoS-атак, защиты интернета и распределенного сервера доменных имен.

Итальянская компания заявила, что клиенты Cloudflare незаконно смотрят много телепередач и потребовали от Cloudflare убрать или отключить доступ к таким сайтам.

В таких случаях итальянское законодательство требует, чтобы поставщик услуг посредников в интернете должен прекратить или предотвратить нарушение только по распоряжению национального суда или компетентного органа административной власти.

В 2020 году подобный иск был подан национальной футбольной лигой и Sky Italy из-за незаконной потоковой трансляции футбольных матчей. В этом случае средство правовой защиты было сложно применить, поскольку от Cloudflare потребовали отключить услуги сети передачи данных для некоторых ее клиентов. Следующий слайд, пожалуйста.

Каким же образом создается сеть в интернете? Сеть в интернете организована как проект, организованный обществом интернета, который обязан своим успехом не только технологиям, но и тому, как он работает и развивается.

Мы много чего можем делать через интернет. Мы можем учиться, объединяться, делиться информацией и организовываться. Это все возможно благодаря тому, что

интернет растет и нам нужно понимать, чем интернет может быть полезным для каждого. Общество интернета определило пять критически важных свойств, которые скорее этические, нежели технические. Следующий слайд, пожалуйста.

Итак, первым свойством является доступность. Другими словами, в какой стране вы бы ни находились, вы всегда можете подключиться к глобальной сети. Вам только нужно устройство и точка доступа, и вы в интернете. Вы можете связаться с любым человеком в мире.

Второе свойство — открытость и функциональная совместимость. Предлагаю думать об интернете как о домике из конструктора ЛЕГО. Мы можем поставить любой блок на платформу и всегда быть уверенными в том, что он всегда подойдет, то есть мы всегда и везде можем беспрепятственно использовать инновации.

Третье свойство — децентрализация. Мы знаем, что интернет — это своего рода «сеть сетей» Каждая независимая сеть подключается к другой и все они выигрывают от возможности подключения к одной сети.

Четвертое свойство — общие глобальные идентификаторы. Другими словами, общий язык для понимания IP-адресов и способа доставки пакетов данных из одной точки в другую.

Пятое свойство не требует особого представления, потому что это — сетевой нейтралитет. Следующий слайд, пожалуйста.

В моей стране практикуется борьба с онлайн-пиратством, заключающаяся в том, чтобы требовать через суды отключения как активных пиратских сайтов так и тех, которые появятся в будущем, которые могут включать те же домены второго уровня. Мы называем их псевдонимами.

Другими словами, какой бы домен верхнего уровня не использовал этот домен второго уровня, существующий или будущий, его нужно отключить. Это необычно еще и потому, что динамические судебные постановления являются самоисполняемыми. Когда нарушающее содержимое зеркалируется на альтернативном сайте с тем же именем домена второго уровня, владельцу прав на интеллектуальную собственность не требуется еще одно судебное постановление. Он обращается напрямую к посреднику, предоставляющему услуги интернета, и просит их отключить их.

Динамическое судебное постановление влияет на еще не существующие нарушения и сайты, которые могут отображать законный контент. И, прежде всего, если операторы инфраструктуры не выполняют постановление, их могут признать ответственными за ущерб. Следующий слайд, пожалуйста.

В данном случае Cloudflare по постановлению суда должны были целевым образом отключить сервис сети передачи данных, а именно конкретные IP-адреса или доменные имена.

Сейчас я хочу показать, какие из пяти критически важных характеристик нарушаются в данном случае. Я также проанализировала 2 и 3 характеристики, но знаю, что этот случай точно нарушает 5 характеристику, а именно сетевой

нейтралитет, поскольку операторы инфраструктуры не могут считаться ответственными за контент, который их клиенты посылают через интернет, и их нельзя просить контролировать данные и выполнять целевую доставку контента.

То же самое, по нашему мнению, произошло на прошлой неделе с поставщиком услуг сети передачи данных Fastly. Многие из наших сайтов не работали в течение часа. Следующий слайд, пожалуйста.

А теперь мой призыв к действию. Эту проблему стоит обсудить на каждом уровне — на форуме по формированию политики ICANN, в сообществе ICANN, на Форуме по управлению интернетом IGF, несмотря на то, какие именно сообщества или заинтересованные стороны затрагиваются таким решением или случаев, как в моей стране, потому что я знаю, что другие юрисдикции также пытаются вдохновиться этой практикой.

Я собираюсь начать анализ того, обсуждались ли связанные проблемы в рамках GNSO и, в особенности группой интересов интернет-провайдеров и группой интересов по вопросам интеллектуальной собственности, чтобы понять, что они делают, думают и знают ли об этом. Если же нет, если сейчас здесь есть представители этих групп заинтересованных сторон, прошу их обратить внимание на эту проблему.

Мое время, похоже, истекло, поэтому попрошу Дебору перейти к следующему слайду и буду заканчивать. Спасибо за то, что выслушали меня.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Вероника. Хорошо поработали. У нас есть вопросы к Веронике? Я не вижу никаких рук или вопросов в чате. Отличная работа, Вероника. Не хочу пропустить их снова. Хорошо. Прекрасно. Хорошая работа. Переходим к нашему следующему докладчику. Это Шивам Шарма. Здравствуйте, Шивам, слово вам. У вас 10 минут. Прошу говорить медленно и четко. Спасибо.

ШИВАМ ШАРМА (SHIVAM SHARMA): Я хочу поговорить о кибербезопасности в отношении устройств интернета медицинских вещей. Следующий слайд, пожалуйста. Что такое интернет медицинских вещей? Это сеть, объединяющая медицинские устройства. Это подраздел технологии «интернет вещей». Речь идет о группе медицинских устройств, включающей датчики и медицинские [неразборчиво] приборы, подключенные к интернету и отправляющие данные пациентов в облако для удаленного доступа медиком или врачом с целью сокращения вероятности [неразборчиво]. Следующий слайд, пожалуйста.

Вот некоторые из таких устройств: трекеры для отслеживания показателей, такие как смартчасы, фитнес-браслеты и клинические устройства для контроля состояния диабетиков и кровяного давления. Вот такие медицинские носимые устройства.

Далее идут цифровые таблетки. Это таблетки, содержащие датчики и вводимые в тело пациента перорально [неразборчиво] для отправки данных за пределы тела пациента и их просмотра с помощью таких устройств, как

смартфоны или планшеты, с помощью которых врач может получить [неразборчиво] больше информации о том, что именно происходит внутри организма.

Далее — автоматические инвалидные коляски. Речь идет об инвалидных колясках с автоматическим управлением. И телемедицина. Благодаря телемедицине для визита к врачу физическое присутствие больше не требуется. В данном случае к врачу можно физически не ходить. Достаточно нескольких киосков или других сервисов телеконференций, посредством которых врач может осматривать пациентов и консультировать удаленно.

Дальше у нас камера для съемки глазного дна. Есть контактные линзы, которые, при установке в глаз, отправляют все данные на смартфон или другое мобильное устройство. Далее идут роботизированные хирургические инструменты. Эти устройства, в основном используются для эндо- и лапароскопических операций. Поставщик услуг или врач могут посредством стримингового сервиса заглянуть внутрь тела и осмотреть организм изнутри с помощью камер.

Это мобильное устройство для анализа патологий. Для анализа не нужно приходить в лабораторию — для сбора данных пациента достаточно использовать определенное устройство у него дома. Например, если нужно выполнить анализ крови, образец можно взять дома и устройства соберут все данные и загрузят их в облако, откуда врач их сможет извлечь.

Следующий. Вот некоторые [неразборчиво] Следующий слайд, пожалуйста.

ДЕБОРА ЭСКАЛЕРА: Шивам, простите, что перебила. Вы можете отрегулировать громкость на своем компьютере или гарнитуре? У нас тут много статических шумов и обратных сигналов. Я не понимаю, что происходит.

ШИВАМ ШАРМА: Извините. Давайте, я возьму другую гарнитуру.

ДЕБОРА ЭСКАЛЕРА: Хорошо, спасибо. Шивам, вы используете гарнитуру?

ШИВАМ ШАРМА: Да.

ДЕБОРА ЭСКАЛЕРА: Да, хорошо. Спасибо.

ШИВАМ ШАРМА: Меня слышно?

ДЕБОРА ЭСКАЛЕРА: Пожалуйста, продолжайте. Спасибо.

ШИВАМ ШАРМА: Теперь посмотрим на архитектуру интернета медицинских вещей. Речь, в основном, идет о разных датчиках, которые [неразборчиво] в тело пациента (датчики жизненных показателей, давления крови, диабетических показателей или

фитнес-браслеты) для сбора данных и их отправки в устройство для дальнейшей передачи через Wi-Fi или, например, 4G или 5G в облако, откуда врач их сможет извлечь для удаленной консультации. Следующий слайд, пожалуйста.

Если взглянуть на рост этой ниши, по отчету AllTheResearch в 2018 году рынок интернета медицинских вещей составлял 44 000 млн, и в период с 2016 по 2026 год ожидается прирост на 24,4% ежегодно. По прогнозам в 2026 году его объем составит около 254 млрд долл. США.

Таким образом, на протяжении прогнозируемого года категория носимых смарт-устройств, вероятно, станет доминирующей на рынке. В 2018 году на мировом рынке интернета медицинских вещей носимые смарт-устройства доминировали и их доля составляла примерно 27%. Комплекты для оказания помощи в полевых условиях показали самый большой совокупный темп годового роста — 30% на мировом рынке интернета медицинских вещей, а для приложений для отслеживания показателей в реальном времени, по прогнозам, этот показатель увеличится на 25%. Для приложений для отслеживания и уведомления рост этого показателя составит 21%. Речь идет о совокупном годовом росте. Следующий слайд, пожалуйста.

Интернет медицинских вещей предлагает ряд преимуществ, таких как сокращение медицинских расходов. Итак, допустим, что пациент страдает от какого-то распространенного заболевания или болезни, не требующей немедленной госпитализации, и врач может консультировать его через интернет. Все данные будут отправляться в облако. Из облака

врач будет получать отчеты, и проводить консультации удаленно. Это уменьшит вероятность госпитализации и сократит расходы.

Также это облегчит жизнь пациенту. Ведь ему или ей не придется ни о чем беспокоиться и даже лично посещать врача. Также следует отметить оптимизацию управления медицинскими препаратами и контроль соблюдения медицинских указаний. Эти средства обеспечат необходимую управляемость, поскольку смарт-устройства способны управлять всем автоматически и обеспечивать эффективное взаимодействие, сокращая также количество ошибок благодаря своей высокой точности. Таким образом, мы получаем лучшие результаты и лучший контроль за расходами в сфере здравоохранения, поскольку в этой сфере много лишних затрат. Это также позволит сократить некоторые виды [неразборчиво] и повысить эффективность предоставляемых услуг, а значит и улучшит результаты лечения. Следующий слайд, пожалуйста.

Если говорить о недостатках интернета медицинских вещей, следует отметить нарушения безопасности или кибератаки, поскольку по мере роста использования интернета растет и их вероятность. Речь идет о таких атаках и заражении устройств вирусами.

Также сложности возникают и в связи с управлением электронными медицинскими картами пациентов, так как при сборе данных пациентов мы должны выполнять ряд требований, таких как стандарты HIPAA, FHIR, а это затратно по времени. В Европе также есть ряд норм, таких как регламент GDPR, которые также нужно выполнять. Также есть и другие

медицинские стандарты, такие как FHIR и SMART. Внедрение всего этого требует времени. Следующий слайд, пожалуйста.

Если говорить о рисках, связанных с интернетом медицинских вещей, следует отметить, что эти устройства имеют длительный цикл разработки: недостаточно просто произвести устройство, но нужно также обеспечить его постоянное обновление через какие-то пакеты исправлений и обновлений для повышения его защиты.

Основная цель этих устройств заключается в обеспечении безопасности пациента, а не защиты, но, в условиях современного мира, нужно обеспечить еще и защиту. Вот пример некоторых таких устройств: Fitbit, использующий Bluetooth для обмена данными, а значит уязвимый для хакеров. Мы можем собирать все данные пациентов, включая местонахождение и все показатели состояния здоровья, которые могут привести к нанесению урона пациенту.

Некоторые из таких устройств имеют зашитые пароли, что тоже таит в себе опасность, поскольку хакерам не составит труда их взломать, если им попадут такие устройства в руки, и получить все данные из них.

И незашифрованный обмен данными. Обмен данными выполняется в незашифрованном формате, из-за чего возрастает вероятность того, что данные будут получены третьими сторонами, например, при атаке посредника.

Далее недостаточно эффективное управление устройствами. Для управления этими устройствами нужно выполнять все требования и постоянно обновлять их все, а наш персонал

должен проходить необходимое обучение, чтобы знать, что делать в случае кибератаки или кибернарушения. Следующий слайд, пожалуйста.

Вот некоторые атаки, которые могут быть предприняты в отношении таких устройств.

ДЕБОРА ЭСКАЛЕРА: Шивам, ваше время истекло, так что, пожалуйста, заканчивайте. Спасибо.

ШИВАМ ШАРМА: Хорошо. Вот эти атаки. Не буду объяснять их, потому что мало времени. Это клонирование меток, взлом и перехват. Следующий слайд, пожалуйста.

Как повысить защищенность таких устройств? Мы не должны использовать [неразборчиво] пароли для устройств, а обновлять их и делать надежными, своевременно предоставлять пакеты исправлений, чтобы своевременно устранять уязвимости безопасности и защищать сеть от несанкционированного доступа. Также не следует забывать, что наши сотрудники могут использовать эти устройства в несанкционированных целях, то есть нужен белый список в соответствии с требованиями. Например, если сотрудник перестанет использовать устройство, мы должны сделать так, чтобы он не имел к нему доступа и иметь возможность круглосуточно отслеживать устройства в режиме 24/7, чтобы вредоносные действия можно было немедленно остановить после их начала.

Далее — недостаточно эффективное сдерживание. [Недостаточно просто отражать атаки.] Для защиты инфраструктуры мы должны устранить атаку до того, как она состоится. Следующий слайд, пожалуйста.

В будущем могут возникнуть задачи, требующие оптимизации медицинской инфраструктуры, так что устройств в ближайшие годы может стать больше. Это все. Большое спасибо за то, что уделили время. Если у вас есть вопросы, задавайте их, пожалуйста.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Шивам. Похоже, Риккардо поднял руку. Риккардо, ваш вопрос?

РИККАРДО НАННИ: Спасибо. Шивам, спасибо за очень хорошую презентацию. Я не специалист в интернете вещей, но мне интересна эта тема и я читал, что интернет вещей способствовал развитию технологий сетевого подключения без IP. Этот тип подключений имеет те же проблемы, что и подключение через IP или интернет вещей имеет другие проблемы? Спасибо.

ШИВАМ ШАРМА: Вы можете задать вопрос в чате? Моя гарнитура, кажется, не работает.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо. И Даниил, вы можете сделать так же? Мы немного перебрали времени и у нас осталось всего несколько минут, поэтому хочу дать слово Риккардо для презентации и вопросов. Итак, Даниил, если вы можете опубликовать свой вопрос также и в чате, это будет отлично.

Последним нашим докладчиком будет Риккардо Нанни. Риккардо, вы следующий. Пожалуйста, помните, что у вас 10 минут, после будет еще пять минут на вопросы. Спасибо, Риккардо.

РИККАРДО НАННИ: Спасибо за возможность выступить. Прошу прощения — у меня нет гарнитуры, но я попытаюсь уменьшить обратный сигнал с помощью наушников. Я буду говорить о фрагментации интернета с общего уровня до конкретного примера, а затем снова вернусь к общим выводам. Следующий слайд, пожалуйста.

Давайте начнем с определения понятия сегментации. Существует много определений этого понятия, например — разная доступность информации и услуг в разных местах под разными правилами. Это, разумеется, очень общий термин. Например, разве это не сегментация, когда в Италии и США нам доступен разный контент Netflix? Существуют регуляторные последствия, определенная сегментация рынка, но если речь идет о сегментации интернета, воображение может разыграться.

Некоторые определения направлены на классификацию сегментации — по государственному, коммерческому и техническому признаку, например. Другие пытаются использовать концепцию сетевого нейтралитета и найти ее связь с сегментацией интернета. Также у нас есть самые строгие определения интернета — несовместимость базовых стандартов, протоколов, разные IP-адреса, разные несовместимые протоколы транспортировки, если [неразборчиво] может иметь другое имя, другую метку.

Это все классификация, разные определения сегментации. Я буду говорить о техническом определении и буду называть все прочие явления другим названием. Следующий слайд, пожалуйста.

Позвольте показать, что я имею в виду, когда говорю о сегментации, и объяснить почему, по крайней мере на техническом уровне, можно сохранять оптимизм в отношении того, что интернет останется в общем унифицированным пространством. Хочу показать вам анализ конкретного примера китайских заинтересованных сторон и их участия в ICANN и не только, включая их участие в регулировании уникальных идентификаторов.

Разумеется, если говорить о сегментации, нужно помнить о множестве важных влиятельных сторон, не только о Китае. Например, о России, о которой мы сегодня говорили, и также, по мнению некоторых людей, о некоторых проектах, созданных в США и нацеленных на сегментацию интернета. Китай я взял только в качестве примера, поскольку он относится к моему географическому региону деятельности и в нем он самый сильный.

Если речь идет о китайских заинтересованных сторонах, становится очевидным, что в начале истории ICANN Китай проявлял ей большое противостояние. После принятия Тайваня в GAC в той форме и под именем китайское правительство прекратило участие в деятельности ICANN. Но остались частые или общественные организации и даже спонсируемые государством.

Затем в течение многих лет китайские заинтересованные стороны и китайское правительство продолжили участие в ICANN и сильно поддерживали интернационализированные доменные имена, что, разумеется, во многом делается в интересах, экономических, политических и культурных, в пространстве имен с китайскими символами.

Первоначально между ICANN и Китаем были споры относительно того, кто должен руководить этим пространством. Даже были опасения, что Китай учредит отдельную систему доменных имен. Однако этого не произошло и, на данный момент, китайские заинтересованные стороны полностью участвуют в работе ICANN и интернационализированных доменных именах.

Здесь мы видим [неразборчиво] между ICANN и Китаем. Китай снова принимает полное участие в работе GAC и принимал заседание ICANN в Пекине в 2013 году, а в 2014 тогдашний президент управления киберпространством Китая одобрил концепцию участия многих заинтересованных сторон на ICANN50. Следующий слайд, пожалуйста.

Это, разумеется, повлияло на позицию китайских заинтересованных сторон в отношении аспектов, связанных с сегментацией интернета и регулированием уникальных идентификаторов. Мы видим, например, что после передачи координирующей роли IANA представитель Китая в GAC стал вице-президентом, что стало сигналом о более активном участии китайского правительства. В то же самое время китайские заинтересованные стороны, даже частные, такие как Huawei, стали все более влиятельными в других областях, связанных с критически важными интернет-ресурсами и уникальными идентификаторами, такими как IETF.

Однако возникли новые геополитические парадоксы в ITU, многоуровневом объекте, когда Huawei, министерство промышленности и информационных технологий и другие влиятельные китайские игроки презентовали так называемое предложение по IP-адресам.

Однако, несмотря на все непонятные моменты, китайские заинтересованные стороны все больше участвуют в работе ICANN, как мы видим. На следующем слайде я продемонстрирую последствия этого. Следующий слайд, пожалуйста.

Итак, что мы имеем на данный момент: после всех лет конфронтации китайские заинтересованные стороны, включая правительство Китая, стали больше участвовать в работе ICANN. Они используют ту же систему доменных имен и протоколы, что и другие страны. Они участвуют в ICANN. Они имеют влияние в IETF. И, если пропустить всю методологию, то должен сказать, что я, в основном, использовал количественные методы, включая интервью экспертов, для сбора данных.

Это случилось благодаря тому, что влиятельные мировые компании, влиятельные игроки, хотят иметь преимущества, предоставляемые присутствием в сети. Различие в стандартах заставляет компании, такие как Huawei, производить разные устройства для разных рынков, чтобы их можно было использовать в разных стандартах, хотя глобальной компании намного проще производить устройства одного типа, которые можно использовать по всему миру. Это намного более прибыльно.

Такие страны как Китай и Россия могут наращивать свое влияние на внутреннее регулирование: что может выходить в интернет, какие действия граждане могут выполнять в интернете для влияния на политику, стандарты, способствующие успешности местных компаний. Именно этим, как кажется некоторым, и занимается Китай в ICANN, IETF и в отношении критически важных интернет-ресурсов и управления интернетом в целом. Следующий слайд, пожалуйста.

Сегодня мы видим, что техническая сегментация интернета стала оружием слабых, тогда как сильные игроки предпочитают сохранить преимущества присутствия в сети. Они могут управлять трафиком, в особенности в отношении распространения информации и организации гражданского общества. Что же касается технических стандартов, они хотят иметь возможность производить одинаковые устройства везде, продавать их по всему миру и сохранить [неразборчиво] преимущества присутствия в сети.

Что нам это говорит о сегментации интернета? Это нам говорит, что самые влиятельные игроки пытаются сохранить унифицированность интернета и только слабейшие могут пытаться сегментировать его на техническом уровне. Это делает интернет и IP, TCP/IP, самое техническое ядро интернета, очень устойчивой средой. В конце концов, Китай имеет сильную цензуру, но, на техническом уровне, для ее обхода достаточно VPN. Использование VPN, разумеется, может быть очень опасным с политической точки зрения, если вы принадлежите к определенным группам, например, к уйгурам. Однако на техническом уровне достаточно VPN.

Так что, это отличные новости для интернета — он может остаться унифицированным на техническом уровне. Несмотря на все остающиеся спорные, неясные вопросы и геополитические конфликты, в отношении основных аспектов интернета, даже на техническом уровне, система обладает определенной устойчивостью. Следующий слайд, пожалуйста.

На этом закончу. Спасибо за внимание. С радостью отвечу на ваши вопросы.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо, Риккардо. Есть ли вопросы к Риккардо? Есть поднятые руки или вопросы в чате? Даниил, говорите.

ДАНИИЛ ГОЛУБЕВ: Риккардо, спасибо за вашу замечательную презентацию. Она была очень информативной и емкой. Есть ли у вас какие-либо прогнозы относительно будущего состояния сегментации? Как вы думаете, унификация интернета будет превалировать или вы не столь оптимистичны и, по вашим прогнозам, некоторые сегменты будут изолированы и отделены? Спасибо.

РИККАРДО НАННИ: Спасибо за вопрос. Это очень хороший вопрос. Я бы сказал, что мы будем наблюдать определенную сегментацию рынка, так как многие западные страны не хотят, например, китайских игроков в своей инфраструктуре, в частности более связанной с телефонией, такой как, например, 5G, и наоборот. Так что да, сегментация рынка возможна. Однако, если речь о стандартах, я вижу тенденцию на схождение, как для IP и DNS, так и для 5G, например.

В случае 3G было много несовместимых региональных или национальных стандартов. Даже если они признавались ITU, они внедрялись только на местном уровне и не работали со стандартами того же поколения, внедренными в других странах, и даже признанными ITU. Сейчас в этой сфере схождение намного более сильное. Есть три утвержденных ITU функционально совместимых, по крайней мере по словам ITU, стандарта 5G.

Таким образом, можно говорить о сходимости стандартов, поскольку, как я говорил, большие компании хотят производить устройства для всего мира, а не использовать собственные стандарты. Им нужна возможность патентовать общемировые

технологии и продавать устройства и сети везде в рамках глобальной экономики.

Но, в то же самое время, правительства осуществляют коммерческую сегментацию, и мы наблюдаем тенденцию ужесточения регулирования. Это так в России и Китае, где правительства становятся все более и более влиятельными в отношении цензуры, регулирования локализации данных. В Европе и США, администрация Трампа, также есть много инноваций — посмотрите на проект «Чистая сеть», например. В Европе, в качестве примера, можно привести регламент GDPR — очень передовой регламент защиты данных, имеющий также и сильный экстерриториальный эффект.

Для меня, как для гражданина ЕС, это, конечно, очень полезно. Я чувствую сильную защиту благодаря регламенту GDPR, так что я абсолютно поддерживаю его и не критикую. Но я хочу сказать, что ЕС также пытается оказывать определенное влияние на цифровой рынок и будущее развитие цифровых технологий, что также включает будущие стандарты интернета, поскольку они будут влиять на будущее развитие искусственного интеллекта, например, и наоборот. Искусственный интеллект также глубоко связан с 5G — 5G способствует развитию искусственного интеллекта, и наоборот — искусственный интеллект используется в сетях 5G.

Если вы сильно контролируете данные, вы также оказываете сильное влияние на развитие искусственного интеллекта, так как данные — наше сырье.

Я о сильном вмешательстве государства на регуляторном уровне, возможно также и в отношении контроля информации, как в Китае и России, насколько я понял, например, но я эксперт не по России. А по сходимости стандартов. Надеюсь, я ответил на ваш вопрос. В некоторых аспектах это была настоящая карусель.

ДАНИИЛ ГОЛУБЕВ: Да. Большое спасибо.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Чудесно. У нас пошел новый час. Спасибо, Риккардо. Отличная презентация. Всем сегодняшним докладчикам из NextGen хочу сказать — отличная работа! Я так горжусь всеми вами. Вы проделали огромную работу.

Хочу поблагодарить всех за то, что присоединились к нам сегодня. Спасибо Фернаде Лунс за слайды. Спасибо нашим переводчикам и, разумеется, нашей фантастической технической команде, помогающей нам с каждой встречей. И, пожалуйста, присоединяйтесь ко второй части презентаций NextGen завтра — в 8:30 по UTC или в 10:30 по CEST. Благодарю всех. Благодарю вас за поддержку и участие в сегодняшней первой части презентации NextGen. Отличная работа! Чудесно. Благодарю вас за то, что вы сегодня здесь. Если есть вопросы, пожалуйста, отправляйте их на адрес —

ЧЕРИ СТАББС (CHERIE STUBBS): Спасибо, Дебора.

ДЕБОРА ЭСКАЛЕРА: Спасибо. Обращайтесь на Engagement@icann.org, если у вас есть или появятся другие вопросы к нашим докладчикам. Огромное спасибо, что были сегодня с нами.

ЧЕРИ СТАББС: Всем пока.

[КОНЕЦ СТЕНОГРАММЫ]