ICANN72 | Виртуальное ежегодное общее собрание – Презентации NextGen
25 октября 2021 года (понедельник), 10:30 – 12:00 по PDT

ДЕБОРА ЭСКАЛЕРА (DEBORAH ESCALERA): Здравствуйте и добро пожаловать на презентации NextGen@ICANN 72. Меня зовут Дебора Эскалера, я руковожу программой NextGen@ICANN. На этом заседании я выступаю менеджером дистанционного 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.

Перевод этого заседания будет осуществляться на английский, французский и испанский языки. Нажмите значок перевода и выберите язык, на котором хотите слушать это заседание.

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 говорить, убедитесь, что вы выбрали язык, на котором будете говорить, в меню перевода. 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. Используйте раскрывающееся меню раздела чата и выберите «Ответить всем докладчикам и участникам». После этого все смогут увидеть ваш комментарий. Обратите также внимание, что в формате вебинара Zoom закрытые чаты возможны только между участниками группы. Любое сообщение, отправленное экспертом панельной дискуссии или обычным участником другому эксперту или обычному участнику, будет видно только организатором заседания, со-организатором и другими экспертами панельной дискуссии.

А сейчас я хотела бы поприветствовать вас на заседании и поблагодарить участников программы NextGen за проделанную работу по подготовке презентаций. Также хочу поблагодарить менторов, Эриса Игнасио (Aris Ignacio) и Дессалина Йехуала (Dessalegn Yehuala), которые в течение последних восьми недель неустанно работали со студентами, помогая им пройти этот процесс и подготовиться к ICANN 72. Они действительно много работали, и без них я бы не справилась.

Кроме того, хочу поблагодарить мою коллегу, Сирануш Варданян (Siranush Vardanyan), которая сегодня будет показывать слайды. Очень признательна вам за помощь, Сирануш. Итак, поскольку у нас всего 90 минут и шесть презентаций, сразу приступим к делу, и я передаю слово нашей первой докладчице Саре Алсамман (Sarah Alsamman). Сара, вам слово, а затем перейдем к вопросам.

САРА АЛСАММАН: Здравствуйте. Большое спасибо, Дебора. Здравствуйте. Спасибо, что пригласили меня. Сегодня я хочу поговорить о злоупотреблении DNS и веб-контентом, а точнее, о дезинформации. Следующий слайд, пожалуйста.

Для тех, кто, возможно, еще не знает, DNS или система доменных имен — это комплексная система, непосредственно от которой зависит подключение пользователей и устройств в сети интернет. Однако, как и в других системах, в ней не исключена возможность злоупотреблений. Как заявил собственный Правительственный консультативный комитет корпорации ICANN, те, кому доверено управление инфраструктурой DNS, должны принять меры по обеспечению безопасности этого общественного ресурса.

Важно, чтобы общественность могла доверять интернету и полагаться на него при осуществлении ответственных коммуникаций и операций. Поэтому мои цели в данной презентации — вовлечь сообщество заинтересованных сторон в диалог по этому важному вопросу общественной политики, а

также призвать сообщество ICANN продолжить борьбу со злоупотреблениями в DNS, с DNS и вокруг DNS в целом.

Однако для того, чтобы должным образом решить проблему злоупотребления DNS, у регистраторов и регистратур должно быть общее понимание того, каким образом его определять. Следующий слайд, пожалуйста. Итак, согласно концепции рабочей группы Internet & Jurisdiction Policy Network, уже выявлено пять основных форм злоупотреблений DNS. Это - вредоносное ПО, ботнеты, фишинг, фарминг и спам.

Существует также злоупотребление контентом, которое не является техническим и поэтому должно быть выделено особо. Для обеспечения защиты свободы слова регистраторы и регистратуры, как правило, не обязаны принимать меры в отношении злоупотреблений веб-контентом. Однако концепцией GAC установлено, что есть особые случаи, когда меры следует принимать, и это касается материалов о сексуальном насилии над детьми, незаконного распространения наркотиков в интернете, торговли людьми, а также конкретных и явных призывов к насилию. Следующий слайд, пожалуйста.

Итак, мы дали определение злоупотреблению контентом в DNS, теперь я хочу поднять вопрос о ботнетах, действующих в социальных сетях. Я уверена, все мы сегодня наблюдаем, как алгоритмы обработки данных становятся все более влиятельными инструментами нашего восприятия, нашей реальности. Наиболее

распространены боты, работающие на политических деятелей, способные манипулировать общественным мнением через основные приложения социальных сетей, которыми мы пользуемся каждый день.

Способность ботнета управлять толкованием общественных проблем оказывает непосредственное влияние на восприятие и упорядочение наших собственных социальных и политических реалий. Чаще всего мы видим это на примере вычислительной пропаганды, и исследования — и в их числе то, которое я представлю на следующем слайде, — показали, что она чаще всего появляется во время или после кризиса, искажая информацию и нанося еще больший ущерб вокруг этого конкретного кризиса.

Поскольку периоды кризиса порождают коллективную неуверенность масс, аудитория в этих сетях становится весьма подверженной влиянию. Следующий слайд, пожалуйста.

Так, после взрыва в Манчестере, признанного терактом, британский Journal of Sociology исследовал сообщения в Twitter и Facebook. В одном случае на странице женщины в Facebook был опубликован пост о том, что она приютила более 60 потерявшихся детей. К посту также был прикреплен номер ее телефона, который быстро распространился в Twitter. Информация распространилась настолько, что в итоге в Daily Mail ее назвали «ангелом Манчестера».

Однако проблема в том, что на самом деле это событие не имело места. Это то, что мы называем «призрачным событием». Позднее женщина объяснила в полиции, что она не публиковала этого сообщения и даже не давала свой номер телефона, и заявила, что была потрясена случившимся, поскольку в течение ночи ей поступали многочисленные звонки. Той же ночью имели место еще 28 подобных призрачных инцидентов, усугубивших хаос после взрыва. Следующий слайд, пожалуйста.

В сети в тот вечер имел место еще один инцидент: в Facebook появилось сообщение о том, что в больнице Олдхэм находится стрелок, а внутри заперты люди. Пост появился через несколько минут после взрыва, его скриншоты из Facebook были распространены как минимум в 368 аккаунтах в Twitter. Больница опровергла этот слух, однако ложная информация продолжала циркулировать в самые критические часы после теракта.

Конкретно это «призрачное событие» отвлекало часть бригад скорой помощи, которые были вынуждены выезжать по ложным вызовам. Подобные ситуации ставят под угрозу безопасность широких слоев населения тем, что социальные сети фактически нарушают обмен информацией между службами экстренной помощи и гражданами, которых они обслуживают. Следующий слайд, пожалуйста.

Таким образом, очевидно, что злоупотребления контентом вебсайтов способны поставить под угрозу жизни людей и

гражданскую оборону, поэтому в будущем они должны стать предметом обсуждения в рамках политики. Для обеспечения будущей безопасности интернета и сообщества его пользователей необходимо стимулировать принятие проактивных мер по борьбе со злоупотреблениями в новых или разрабатываемых положениях соглашения об администрировании домена верхнего уровня. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Сара. Хорошо поработали. Хорошо, есть вопросы к Саре? Не вижу вопросов. Если вопросы возникнут, вы всегда можете задать их в конце дискуссии. Тогда мы переходим к нашему следующему докладчику - Мери Багдасарян (Meri Baghdasaryan). Спасибо.

МЕРИ БАГДАСАРЯН: Спасибо, Дебора и Сирануш. Доброе утро, добрый день, добрый вечер! Мери Багдасарян, я недавно окончила магистратуру юридического факультета Университета Пенсильвании. Интерес к конфиденциальности и разработке политики в ICANN привел меня к теме сегодняшней презентации, а именно к теме аккредитации услуг сохранения конфиденциальности и регистрации через доверенных лиц. Следующий слайд, пожалуйста.

В июне 2013 года Правление ICANN утвердило новое Соглашение об аккредитации регистраторов, или RAA, — договор,

регулирующий взаимоотношения между ICANN и каждым из аккредитованных корпорацией регистраторов. Как мы видим, положения этого соглашения могут оказать влияние на владельцев доменов и других третьих лиц, имеющих отношение к системе доменных имен.

Начиная переговоры по этому соглашению между ICANN и группой заинтересованных сторон-регистраторов в октябре 2011 года, Правление ICANN также предложило GNSO подготовить отчет о неразрешенных проблемах, чтобы после завершения переговоров начать процесс разработки политики GNSO для решения проблем, которые не были урегулированы на переговорах. И среди оставшихся были названы вопросы, относящиеся к проблемам услуг сохранения конфиденциальности и регистрации через доверенных лиц.

Соглашение об аккредитации регистраторов 2013 года содержит временную спецификацию, охватывающую обязательства регистраторов в отношении услуг сохранения конфиденциальности и регистрации через доверенных лиц. Срок действия этой временной спецификации уже несколько раз продлевался, и теперь он истекает 31 июля 2022 года или когда ICANN внедрит новую программу аккредитации, в зависимости от того, что произойдет раньше.

Но прежде чем продолжить, давайте разберемся, что мы понимаем под услугой сохранения конфиденциальности и регистрации

через доверенных лиц. В настоящее время они определяются в рамках упомянутой спецификации. Итак, услуга сохранения конфиденциальности позволяет зарегистрировать доменное имя на владельца домена, но все остальные контактные данные, отображаемые в общедоступной службе каталога регистрационных данных, на самом деле предоставляются не владельцем домена, а провайдером услуги конфиденциальности.

Что же касается регистрации через доверенных лиц, эта услуга позволяет владельцу зарегистрированного имени разрешить использование доменного имени клиенту, который фактически использует домен, а контактную информацию в этом каталоге предоставляет провайдер услуги регистрации через доверенных лиц. Следующий слайд, пожалуйста.

Согласно этой спецификации, действующей в настоящее время, у нас есть минимальный набор требований, применимых к услугам сохранения конфиденциальности и регистрации через доверенных лиц. Четыре основных минимальных требования включают раскрытие важнейших условий обслуживания, опубликование сведений о контактном лице для сообщений о нарушениях или злоупотреблениях, опубликование деловых контактных данных и депонирование данных клиентов. Как мы видим, спецификация пытается решить проблему обработки этих непубличных регистрационных данных. Следующий слайд, пожалуйста.

Но почему мы вообще обсуждаем этот вопрос? Почему это важно? Если вернуться к 2011 году, когда Правление ICANN запросило отчет о неразрешенных проблемах у GNSO, Правление ICANN также подчеркнуло важность незамедлительного решения этой проблемы с помощью услуг сохранения конфиденциальности и регистрации через доверенных лиц, поскольку это обеспечит повышенную защиту для владельцев доменов и снизит число злоупотреблений DNS.

С тех пор проблема действительно стала хронической и даже обострилась во время пандемии. Например, во время конференции ICANN 68 на заседании GAC, посвященном злоупотреблениям DNS, было отмечено, что 65% доменов, использовавшихся для обмана людей во время пандемии, были скрыты с помощью услуг сохранения конфиденциальности и регистрации через доверенных лиц. Более того, некоторые практикующие юристы также забили тревогу по поводу того, что после вступления в силу GDPR количество жалоб ВОИС в отношении UDRP против нарушителей DNS значительно возросло, и большинство этих жалоб связано с постоянным несоблюдением требований по раскрытию контактной информации со стороны провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц. В результате регистраторы или аффилированные с провайдеры услуг регистрации через доверенных лиц требуют от владельцев IP подавать иски в рамках UDPR или требовать повестку с вызовом в суд, чтобы получить

контактную информацию лица, совершающего злоупотребления DNS.

Очевидно, что это вызывает множество ненужных проблем, связанных с необходимостью тратить больше времени на прохождение простой процедуры, и больше ресурсов на получение контактной информации для дальнейшего рассмотрения жалоб. Другими словами, аккредитация действительно поможет повысить защиту владельцев доменов, чтобы уменьшить злоупотребления DNS, а также снизить количество жалоб по UDRP. А теперь вернемся к запросу Правления ICANN о предоставлении отчета от GNSO и поговорим о том, что произошло после [этого]. Следующий слайд, пожалуйста.

Итак, на этом слайде мы видим обзор процесса разработки политики GNSO, или PDP. После утверждения Правлением соглашения об аккредитации регистраторов в 2013 году GNSO инициировала PDP и в том же году сформировала рабочую группу.

Рекомендации по политике были приняты Советом GNSO в январе 2016 года и утверждены Правлением ICANN в августе 2016 года. После этого Правление поручило реализацию рекомендаций корпорации ICANN. Следующий слайд, пожалуйста.

И новая программа аккредитации, как мы видим на слайде, на самом деле содержит более детализированные требования, чем спецификации, которые мы уже обсуждали. И на основании того, что вы видите на экране, становится ясно, что новая программа

пытается решить вопросы, связанные с услугами сохранения конфиденциальности и регистрации через доверенных лиц.

Например, она дает детальную основу для ответов провайдеров на запросы правоохранительных органов и владельцев интеллектуальной собственности, или стандартизирует требования к передаче провайдерами сообщений от третьих лиц тем, кто пользуется услугами сохранения конфиденциальности и регистрации через доверенных лиц, и даже предусматривает обязательную образовательную программу для провайдеров.

Таким образом, как мы видим, новая программа пытается решить проблемы с текущей спецификацией, чтобы обеспечить более прозрачную и разумную основу для аккредитации. Следующий слайд, пожалуйста.

Как я уже упоминала, после того как Совет GNSO принял рекомендации рабочей группы, Правление ICANN их утвердило и направило в корпорацию ICANN для реализации. Ожидалось, что новая программа аккредитации заменит спецификации по соглашению об аккредитации регистраторов. Однако в настоящее время реализация этой программы приостановлена, и причиной тому — усилия ICANN по приведению текущей практики защиты данных в соответствие с Общими положениями о защите данных Европейского Союза.

Если вернуться немного назад, то в июле 2018 года, после принятия Правлением ICANN решения одобрить Временную

спецификацию для регистрационных данных в gTLD, Совет GNSO инициировал и учредил ускоренный процесс формирования политики или EPDP, который стал первым EPDP в истории ICANN.

Позже, в марте 2019 года, Совет GNSO принял отчет, первый отчет рабочей группы о первой фазе EPDP, 27 из 29 рекомендаций которого были позже одобрены Правлением ICANN. Однако, согласно рекомендации 27 из отчета о первой фазе, стало ясно, что с учетом этих новых событий в свете более соответствующей GDPR практики в ICANN, возникла необходимость пересмотреть все соответствующие практики, которые также связаны с любыми не общедоступными регистрационными данными.

Вот почему эта программа пока приостановлена в ожидании комментариев от сообщества и проверки, и, по сути, если подумать, EPDP и рекомендации по программы аккредитации преследуют одну и ту же цель, которая заключается в определении законного механизма доступа к не общедоступным регистрационным данным и обращения с ними. Следующий слайд, пожалуйста. Поэтому после возобновления реализации мы ожидаем запроса комментариев сообщества по следующим документам. Следующий слайд, пожалуйста.

Комментарии сообщества будут запрошены в отношении политики аккредитации услуг сохранения конфиденциальности и регистрации через доверенных лиц, соглашения, руководству кандидата программы, а также процедурам приостановления,

отмены и передачи аккредитации. Короче говоря, мы видим, что аккредитация услуг сохранения конфиденциальности и регистрации через доверенных лиц — это важный вопрос, который прошел через процесс разработки политики ICANN. Но, будучи частью большей головоломки в работе ICANN по обеспечению соответствия практики GDPR, реализация программы аккредитации приостановлена, и, с точки зрения рекомендаций EPDP, [необходимо] согласовать проекты, чтобы сложились все части головоломки.

В любом случае, у программы аккредитации более детализированный подход, чем текущие требования спецификации. Тем не менее, основные проблемы с услугами сохранения конфиденциальности и регистрации через доверенных лиц, похоже, не только не исчезли, но даже, как я уже упоминала, обострились во время пандемии. Поэтому, принимая во внимание важность программы, я надеюсь, что реализация пойдет достаточно быстро, чтобы решить основные проблемы. Большое спасибо, и я с нетерпением жду возможности получить больше информации по этой и другим темам на конференции ICANN 72. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Мери. По-моему, в чате есть вопрос. Вот он: «Не могли бы вы немного объяснить, что такое временное депонирование данных в контексте обсуждаемой темы?».

МЕРИ БАГДАСАРЯН: Да. На самом деле на эту тему можно говорить долго, поэтому я могу просто напечатать ответ, если мы хотим продолжить обсуждение. Но в двух словах, речь о том, как в услугах сохранения конфиденциальности и регистрации через доверенных лиц будут обрабатываться любые запросы от правоохранительных органов или владельцев интеллектуальной собственности, и как хранятся и обрабатываются данные в этих сервисах. Это краткий ответ, но в чате я могла бы дать более развернутую версию, если вы не против.

ДЕБОРА ЭСКАЛЕРА: Конечно. Огромное спасибо. Есть ли еще вопросы к Мери? Хорошо, буду следить за чатом. Огромное спасибо. Хорошо поработали. Ладно, тогда мы переходим к нашему следующему докладчику, Саи Чандрасекарану (Sai Chandrasekaran). Саи, прошу вас.

САИ ЧАНДРАСЕКАРАН: Спасибо, Дебора и Сирануш. Это Саи Чандрасекаран, и сегодня я выступлю по теме, которая меня больше всего заинтересовала в ходе моего исследования, а эта тема — модерация контента.

Сегодня мы поговорим о проблемах, возникающих при модерации контента, рисках для конфиденциальности, которые создает модерация контента, и о том, как мы можем решить столь сложную проблему. Следующий слайд, пожалуйста.

Я хочу немного рассказать о себе. Я учусь в аспирантуре по специальности кибербезопасность в Индианском университете, последние несколько месяцев я провожу исследования по ряду тем, имеющих отношение к управлению интернетом, в том числе к модерации контента. Так что на этом форуме я с радостью поделюсь своими соображениями по теме. Следующий слайд, пожалуйста.

Большинство из тех, кто следит за новостями или пользуется социальными сетями, наверняка сталкивались с шумихой вокруг модерации контента. Вы могли видеть, как правительства пытаются пресечь дезинформацию, особенно во время пандемии, как компании-владельцы соцсетей пытаются контролировать угрозы злоупотреблений, как ученые-юристы пытаются создавать правовые прецеденты для решения проблемы модерации контента, как группы по защите конфиденциальности и прав человека выражают серьезную озабоченность тем, что модерация контента угрожает свободе слова и частной жизни. Следующий слайд, пожалуйста.

Я составил краткую хронологию событий, связанных с модерацией контента. Чтобы сэкономить время, не буду рассматривать каждое из этих событий, но остановлюсь на нескольких из них, чтобы показать, почему эта тема актуальна, и что это очень сложный вопрос.

Например, в 2021 году, всего несколько месяцев назад, главный хирург США открыто выступил за то, чтобы попытаться остановить дезинформацию в здравоохранении. Он сказал, что она представляет серьезную угрозу для здоровья населения, и ограничение ее распространения — гражданская и моральной ответственность. Фактически, [невнятно] призвал владельцев социальных сетей [невнятно] выявлять и предотвращать распространение ложной информации.

Нужно понять, что модерация контента — это не локальная проблема, касающаяся только США. Это глобальная проблема. Недавно в Индии был принят ряд законов о цифровых СМИ, которые требовали от провайдеров контента в социальных сетях модерировать контент и отслеживать [невнятно]. И это встретило жесткое сопротивление со стороны компании WhatsApp, которая подала жалобу в суд на эти новые правила.

Всего несколько недель назад бывший сотрудник Facebook давал показания в сенате по поводу оптимизации контента Facebook и ее влияния на общество. Следующий слайд, пожалуйста.

Если вы спросите любого, кто работает в сфере безопасности и конфиденциальности, он скажет, что лучший способ решить проблему и разобраться в ней — это провести оценку рисков. Поэтому я провел оценку рисков конфиденциальности в отношении модерации контента, которая основана на отраслевом

стандарте, отраслевой таксономии, разработанной известным специалистом Дэниелом Солоувом (Daniel Solove).

Предположим, что мы делимся информацией или обмениваемся сообщениями через сервис, поддерживающий сквозное шифрование, например, WhatsApp или Apple Messages. В этом случае у нас, как у пользователей, есть некоторые базовые ожидания в отношении тайны и конфиденциальности сообщений, которыми мы обмениваемся.

Но предположим, что я, как поставщик услуг, с помощью некоего алгоритма определяю, являются эти сообщения опасными или нет, и если это так, [неразборчиво] раскрываю эту информацию инструменту, то в этом случае я в некотором смысле нарушаю личное пространство и конфиденциальность пользователей.

Поэтому необходимо понять одну вещь: как показывает история, всякий раз, когда разрабатывается новая функциональная возможность, мы должны думать не только о том, как мы можем ее использовать, но и о том, как ею можно злоупотребить. Поэтому, принимая во внимание, что эти технологии сканирования, особенно в зашифрованной системе, могут быть использованы правительством и злонамеренными [субъектами, создающими угрозы] для возможной поддержки слежки и прослушивания, что имеет огромные последствия для свободы слова в нашем обществе и является серьезным фактором устрашения.

И еще кое-что, о чем я хотел бы вам сказать: иногда раскрытие информации может быть обратным. Допустим, я — пользователь, и интимные подробности обо мне, такие как сексуальная ориентация и употребление психотропных веществ, попадают в открытый доступ. В этом случае у меня нет никаких мер защиты от тяжкого эмоционального вреда и психического воздействия, вызванного раскрытием информации.

По сравнению, предположим, с разглашением финансовой информации, — это совершенно иной случай. В этом случае вы можете заблокировать кредитную карту, чтобы предотвратить любы отрицательные последствия. Но в данном случае, поскольку раскрывается информация о вашем здоровье, у вас нет таких [невнятно] мер. Следующий слайд, пожалуйста.

Итак, в предыдущем слайде я говорил об угрозах конфиденциальности, которые может вызвать модерация контента. Но в то же время есть некоторые веские аргументы, которые приводятся с другой стороны. Допустим, некоторые люди говорят, что модерация контента может быть использована для прекращения насилия и, в конечном счете, даже для предотвращения смертей, особенно в отношении насилия, как это было в Мьянме.

Поэтому я считаю, что мы можем принять подход к модерации контента, сохраняющий конфиденциальность, в основе которого три ключевых компонента. Первый — технический. Он

предполагает сотрудничество между техническими организациями и образовательными учреждениями для совместной работы и разработки безопасных криптографических методов, выявляющих любую дезинформацию или ложную информацию и в то же время не нарушающих личное пространство и конфиденциальность пользователей.

Например, в данном случае мы можем использовать безопасную многостороннюю криптографическую технику, которая сканирует изображения и сравнивает их с хранилищем изображений, включающим весь перечень злоупотреблений. И если информация не соответствует, изображение не будет передано поставщику услуг.

Еще один важный ключевой компонент, о котором я хочу рассказать, — это процесс, и это то, что я называю моделью информационного надзорного органа. Я хочу, чтобы пользователи с ответственностью подходили к раскрытию провайдерам услуг любой ложной информации, которую они получают, чтобы мы могли создать своего рода модель доверия и активно бороться с дезинформацией.

Последний компонент, о котором я собираюсь рассказать, — это принцип, который заключается в том, что когда у нас будет некоторая степень доверия между заинтересованными сторонами... давайте рассмотрим пример. Если я — провайдер услуг, активно модерировавший контент, то думаю, мне нужно

обеспечить определенную транспарентность в отношении моих алгоритмов, чтобы завоевать доверие всех заинтересованных сторон в этом процессе. Следующий слайд, пожалуйста.

Итак, я перехожу к последнему слайду, и я думаю, что проблема модерации контента очень похожа на проблему изменения климата. Разные страны хотят решить эту проблему. Почти все страны хотят решить эту проблему. Но у них разные способы ее решения. И чаще всего они не идут рука об руку.

И я бы хотел, чтобы для активного решения проблемы модерации контента был применен принцип участия многих заинтересованных сторон, при котором люди ответственно раскрывают любую ложную информацию провайдерам услуг с помощью знаний и инструментов, предоставляемых преподавателями и образовательными учреждениями. Технологические платформы должны решать проблему нехватки информации и уделять приоритетное внимание раннему выявлению [суперраспространителей] и повторно совершающих нарушения, сохраняя при этом конфиденциальность.

И одной из ключевых заинтересованных сторон в этом процессе являются все мировые правительства, которым необходимо обратиться ко всем частным некоммерческим организациям, чтобы найти точки соприкосновения или выработать общий подход к поиску соответствующих правовых и нормативных мер

для решения проблемы модерации контента. Благодарю за ваше время и терпение. Буду рад ответить на любые ваши вопросы.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Саи. У кого-нибудь есть вопросы к Саи? Хорошо. У переводчиков возникли небольшие трудности, но я хочу напомнить всем, что ведется запись этого заседания, и примерно через неделю вы получите к ней доступ. Если кто-то захочет посмотреть запись, у вас будет такая возможность.

Инек, у вас был вопрос? Прошу вас, говорите.

ИНЕК НИКИНГБОУНГ ДУУТ (ENOCH NIKINGBOUNG DUUT): Да. Большое спасибо. Небольшой вопрос по модерации контента. Модерация контента — это некоторым образом двусторонняя проблема. С одной стороны, мы не хотим препятствовать свободе слова и все такое. С другой стороны, мы также хотим исключить контент, который не должен находиться [в общественном] доступе.

Итак, есть ли у нас некое среднее решение, которое снизит риск того, что люди смогут говорить что угодно и где угодно, и в то же время не будет препятствовать свободе слова? К примеру, в традиционных СМИ у нас есть регуляторы. А в социальных сетях могут ли у нас быть независимые регуляторы, которые помогут в этом отношении? Большое спасибо.

САИ ЧАНДРАСЕКАРАН: Спасибо за вопрос, Инек. К сожалению, на данный момент у нас нет готового решения, которое действительно обеспечивало бы баланс между борьбой с дезинформацией и свободой слова. Но, думаю, если вы смотрите новости, то наверняка слышали об инциденте в Apple со сканированием на стороне клиента. Они хотели провести клиентское сканирование на стороне пользователя, чтобы выявить любые изображения, связанные с сексуальным насилием над детьми и т.д., но к этому негативно отнеслось гражданское общество в лице сторонников сохранения конфиденциальности, а также специалистов в области безопасности.

Поэтому, к сожалению, на данный момент у нас ничего нет, но, как я говорил в своей презентации, у нас есть нечто, называемое безопасной многосторонней криптографической техникой, которая фактически сравнивает эти изображения с хранилищем изображений со сценами насилия, и только если информация совпадает, сообщает об этом провайдеру. В противном случае провайдеру информация не передается. Надеюсь, что ответил на ваш вопрос.

ИНЕК НИКИНГБОУНГ ДУУТ: Спасибо. Если можно, разместите это в чате для дальнейшего [невнятно], пожалуйста. Спасибо.

САИ ЧАНДРАСЕКАРАН: Обязательно, Инек. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо за вопрос. Есть еще вопросы к Саи? Хорошо, переходим к следующему докладчику, Кэди Хаммер (Kady Hammer). Кэди, прошу вас.

КЭДИ ХАММЕР: Здравствуйте! Меня зовут Кэди Хаммер, я студентка юридического факультета Американского университета в Вашингтоне. Я буду говорить об очень распространенном среди представителей поколения Z термине «фильтрование», применительно к протоколам шлюзов или, иначе говоря, механизмам безопасности для протоколов шлюзов, в частности, протоколов граничного шлюза. Следующий слайд, пожалуйста.

Сначала вкратце расскажу, как мы здесь оказались и почему я поднимаю вопрос о протоколах граничного шлюза. Сразу поясню, что я не технолог, я студентка юридического факультета. Поэтому мне потребовалось довольно много времени, чтобы разобраться, как работает инфраструктура интернета. Думаю, вы все прекрасно знаете, что интернет создавался в первую очередь для целей коммуникации. Безопасность не всегда была первой или основной проблемой при разработке инфраструктуры интернета. Но в современном мире она становится все актуальнее, особенно

с учетом постоянно растущего числа киберугроз и киберсубъектов.

В 1989 году среди многих других протоколов был разработан протокол граничного шлюза. BGP — так я буду называть его в дальнейшем для простоты — опирается на отдельные сети, которые непрерывно обмениваются между собой информацией о доступных каналах передачи данных, доступных IP-адресах, благодаря чему интернет разросся в огромную глобальную сеть, которую он представляет собой сегодня.

Следует отметить, что BGP не требует аутентификации ни IP-адресов, ни автономных систем, с которыми они взаимодействуют. Вместо этого BGP работает в рамках так называемой системы доверия, или, возможно, вы также знаете ее как «систему чести», в рамках которой сети доверяют, что другие сети являются добросовестными игроками.

В целом, BGP был прост, он позволял решать проблемы в протоколах маршрутизации и обеспечивал достаточно универсальную структуру, которая сохранилась до наших дней. Следующий слайд, пожалуйста.

Итак, здесь представлен общий обзор, диаграмма и список протоколов маршрутизации. Как я уже говорила, BGP — один из многих протоколов маршрутизации. Основная цель протокола маршрутизации — распределение сетевого трафика между другими сетевыми системами, устройствами. Следует отметить,

что он не обеспечивает безопасность при доставке информации. Поэтому, опять же, это возвращает нас к системе доверия или системе чести.

Как вы видите, список типов протоколов маршрутизации длинный. Я не буду вам их зачитывать. А график в правой части экрана дает общее представление о том, как работает BGP или другой протокол маршрутизации, EGP. Вы можете видеть, как сети общаются друг с другом, с автономными системами — это я объясню чуть позже — и просто визуальное представление, если вам это интересно. Следующий слайд, пожалуйста.

Рассмотрим более детально специфику протокола граничного шлюза: BGP — это протокол маршрутизации с вектором пути, который работает между автономными системами в интернете. Вместо того чтобы отслеживать всю карту интернета, маршрутизаторы BGP полагаются на информацию от соседних маршрутизаторов или систем, которые выбирают кратчайший путь для включения в таблицу маршрутизации. Затем каждый маршрутизатор объявляет об этом пути другим соседям, которые ищут эту информацию. И если политика позволяет, они обмениваются этой информацией.

Один тонкий момент: когда мы говорим об автономных системах или сетях, которые BGP использует для связи, вы можете услышать, что они называются автономными системами, что подразумевает наличие одной системы. Однако автономные

системы иногда включают целую организацию, в которую входят несколько маршрутизаторов или устройств. Поэтому этот термин используется для более широкого обозначения в более абстрактном смысле.

Номера автономных систем интернета присваиваются интернет-провайдером, к которому подключаются конечные пользователи, такие как мы, использующие интернет, или иногда они присваиваются регистратурой.

В конечном итоге BGP помогает маршрутизаторам выбрать путь, в частности, кратчайший путь для получения этой информации, и причина, по которой этот протокол так важен, заключается в том, что отслеживание всей системы интернета — это уже само по себе большое достижение. Он полагается на соседние сети для обмена этой информацией, чтобы вы быстрее добрались до нужной информации или сайта.

Причина, по которой это важно, заключается в том, что из-за того, как работает BGP, системы могут быть атакованы вместе. Злоумышленник получает возможность атаковать не отдельное устройство, а целую автономную систему, которая может включать организации, компании и т.д. Следующий слайд, пожалуйста.

Сегодня я хочу поговорить о проблемах безопасности, возникающих в протоколах - спасибо Брайану, который объясняет это в чате, - а конкретнее, о проблемах безопасности,

возникающих в BGP. Хотя эти проблемы безопасности не являются специфическими для BGP, они присутствуют и в других протоколах маршрутизации.

Одна из основных проблем — человеческий фактор. Вспомним инцидент с Facebook, который, хотя проблема Facebook и не была полностью связана с BGP, можно считать примером того, что может произойти. Таким образом, ошибка оператора может случайно привести к неправильным конфигурациям, при которых целая организация или автономная сетевая система может быть выведена из строя или пропасть из интернета и посеять хаос.

Но главное, о чем я хочу поговорить, — это злонамеренное вмешательство. Все протоколы маршрутизации могут быть объектами атак, будь то подмена IP-адреса, перехват сеанса, атаки типа «отказ в обслуживании» и многие другие способы, с помощью которых злоумышленники могут ввести неверную информацию в таблицы BGP.

Например, поскольку BGP полагается на соседние сети, соседняя с вами сеть может оказаться злоумышленником, который вводит неверную информацию в ваш запрос, направляя вас на вредоносный веб-сайт или т.п.

А поскольку маршрутизаторы BGP доверяют друг другу, то, как я уже отмечала, в BGP не существует истинных механизмов аутентификации. И нет способа проверить, кто в данный момент на другой стороне или что говорят другие сетевые системы.

Подтверждена ли информация, достоверна ли она, заслуживает ли она доверия. Еще один момент заключается в том, что криптографическая аутентификация не является обязательной. Это я объясню на следующем слайде.

Чтобы приблизить это к реальности, я хотела бы привести пример, что представляет собой захват BGP и как это произошло через систему DNS Amazon. В 2018 году злоумышленники использовали атаку на BGP (атака «человек посередине») для перенаправления трафика на сервис Route 53 Amazon с помощью сервера в чикагском центре обработки данных IBX, что позволило им перехватывать трафик по всему миру.

В частности, злоумышленники атаковали MyEtherWallet.com, блокчейн-платформу Ethereum, перенаправив трафик клиентов на поддельную или подставную страницу, которая похищала всю информацию клиентов.

Это происходило следующим образом: сетевой трафик перенаправлялся на сервер, расположенный в России, который выдавал себя за веб-страницу MyEtherWallet, используя поддельный сертификат, и похищал криптовпалюту клиентов. Атака требовала доступа к маршрутизаторам BGP интернет-провайдеров и требовала существенных вычислительных ресурсов. Это то, что я хочу отметить. Поскольку они перенаправили весь этот трафик, им пришлось иметь дело со значительным сетевым трафиком, поступающим на их серверы.

Это важно, потому что эта атака подчеркивает наличие проблем безопасности как в BGP и DNS, так и в более широком смысле в различных протоколах маршрутизации. На сегодняшний день это крупнейшая известная атака такого масштаба, в которой проявилась уязвимость BGP и DNS, о чем уже рассказывали другие докладчики из NextGen. На инфографике внизу вы видите, как это могло произойти. Следующий слайд, пожалуйста.

Итак, как обеспечить фильтрование. В целом, есть несколько вещей, необходимых, чтобы рассматривать вопрос о том, как сделать более безопасными протоколы маршрутизации, и в частности, как сделать более безопасными протоколы BGP.

В целом, нам нужно программное обеспечение маршрутизатора, обеспечивающее IPsec, безопасность интернет-протокола. Это можно реализовать с помощью инфраструктуры открытых ключей или цифровых подписей.

Необходимо определить роль, которую играют региональные регистратуры в обязанностях центра сертификации — кто отвечает за префиксы адресов и номера автономных систем, как за их назначение, так и за местоположение.

Важным компонентом, который потребует значительных финансовых вложений, является обновление аппаратной инфраструктуры, включая маршрутизаторы (провайдеров и абонентов), чтобы определить роль провайдеров в сертификации и обработке и сертификации этой информации. Конечно,

обновление физического оборудования подразумевает значительные финансовые вложения.

Необходимо более стратегически и вдумчиво подходить к тому, как совершенствовать BGP в будущем, и особенно необходимо придерживаться подхода, ориентированного на безопасность, чтобы мы были менее реактивны и более проактивны. Также необходимо определить критерии оценки, как мы будем определять, считается ли сеть, маршрутизатор, любое лицо или организация безопасным или проверенным или надежным источником, какие критерии мы будем использовать, чтобы разрешать или не разрешать этим сетям взаимодействовать и работать в экосистеме интернета.

Итак, на экране я представила три решения, и ни одно из них не является новым. Некоторые из них фактически появились при создании BGP в 80-х и начале 90-х годов. Таким образом, уже существуют решения, как мы можем защитить и обезопасить протоколы граничного шлюза.

Один из вариантов — безопасный протокол граничного шлюза, который обеспечивает три конкретных механизма безопасности. Первый — это инфраструктура открытых ключей. Этот механизм будет использоваться для подтверждения подлинности владения IP-адресом или блоком IP-адресов.

Другим вариантом в этом первом решении является атрибут транзитивного пути. Он будет использоваться для передачи

цифровых подписей, которые удостоверяют подлинность информации маршрутизатора. Таким образом, когда эта информация перемещается, в ней присутствует своего рода флажок безопасности. Или, как я уже упоминала, можно использовать безопасность интернет-протокола, который в основном используется для предоставления данных, подтверждающих подлинность информации до обмена информацией через BGP.

Другим механизмом или решением является безопасное происхождение BGP. Это фактически возвращает нас к третьему пункту первого решения. Перед обменом информацией каждая организация должна сертифицировать или быть сертифицированной, поэтому их полномочия должны быть подтверждены. Каждый разрешительный сертификат должен быть подтвержден. Опять же, это возвращает нас к тому, какую роль играют регистратуры, какую роль играют интернет-провайдеры. Информация, содержащаяся в этих сертификатах, также должна соотноситься с более обширной базой данных, в которой будут храниться эти сертификаты. Опять же, какая регистратура или какая заинтересованная сторона интернета будет играть роль в ведении такой базы данных. И опять же, необходимо подумать о безопасности этой базы данных.

Другое решение называется масштабируемый транспорт BGP, оно заменяет TCP, другой протокол маршрутизации, на собственный транспортный протокол. Конкретно это решение может быть не

самым реалистичным, учитывая, что в нем происходит приватизация, но оно использует технику, называемую волновым методом, которая позволяет транспортировать данные, отправляя сообщения о соединении только своим соседям вместо того, чтобы соединяться со всеми сетями или всеми маршрутизаторами в сети. Следующий слайд, пожалуйста.

Очевидно, что в безопасном протоколе граничного шлюза есть свои сложности, поэтому существующие предлагаемые решения еще не проработаны, и поэтому мы все еще это обсуждаем. Итак, основной проблемой всегда являются расходы, которых потребуют эти решения в части инфраструктуры, персонала, координации, распределения ответственности. Таковы ключевые компоненты первых двух решений.

И я уже коснулась последнего решения, но оно требует широкого участия. Если вы меняете целый протокол, это большая работа, и другой аспект — он будет запатентован, поэтому не будет бесплатным, и может не быть доступным, и, в конечном счете, полномочия или механизм контроля уйдут к владельцу.

Кроме того, в целом, одной из наиболее серьезных проблем является самоуспокоенность или отсутствие срочности, пока не грянет кризис. Я уже говорила о реактивном подходе большинства заинтересованных сторон — даже меня в том числе — к собственной безопасности, и мы склонны применять временные, а не упреждающие решения.

Конечно, учитывая долговечность интернета и то, как долго он существует, быть проактивным очень сложно. Другое дело, что эта проблема рассматривается как незначительная, учитывая небольшие масштабы атак, которые имели место. Я отметила, что MyEtherWallet была самой крупной по своим масштабам, хотя ее целью была всего одна компания, но вы можете представить, насколько широкомасштабными могут быть эти атаки и какой ущерб и хаос они могут причинить, если BGP станет одним из новых объектов внимания злоумышленников. Следующий слайд, пожалуйста.

Итак, я затронула почти все пункты, но хочу подчеркнуть одну вещь: хотя это серьезная проблема, мы можем обратиться к существующим моделям того, как мы можем создать заинтересованную сторону и изменить общий подход к обеспечению безопасности BGP. Если мы рассмотрим HTTP и то, как мы перешли от HTTP к HTTPS, мы, вероятно, сможем решить эту проблему. Следующий слайд, пожалуйста.

И это все. Большое спасибо за внимание.

ДЕБОРА ЭСКАЛЕРА: Отличная презентация. И очень интересная. Отлично. В чате шла содержательная беседа. Очевидно, это хорошая, интересная тема, которая очень интересует людей. Есть ли вопросы к Кэди? Отличная работа, Кади, хорошее представление и очень хорошая структура.

Хорошо, если нет других вопросов — и помните, можно присылать вопросы и после заседания, — мы переходим к нашему следующему докладчику, Скотту Киму (Scott Kim). Скотт, вы следующий. Спасибо.

СКОТТ КИМ: Спасибо. Здравствуйте! Спасибо. Здравствуйте! Меня зовут Скотт Ким, я учусь в аспирантуре и работаю специалистом по информационной безопасности. Моя роль заключается в сборе информации, ее анализе и распространении среди соответствующих заинтересованных сторон. Сегодня я хочу поговорить об использовании поиска ICANN для поиска индикаторов компрометации. Следующий слайд, пожалуйста.

Итак, я расскажу о том, что такое APT41, о некоторых тематических исследованиях и, наконец, о рекомендациях.

Группа APT41 не особо известна сообществу, зато хорошо известна специалистам по информационной безопасности. APT41 также известна под разными именами в разных компаниях, поэтому они могут называться Blackfly, Earth Baku, Wicked Panda. APT41 — это спонсируемая китайским государством группа постоянных угроз повышенной сложности, которая проводила кампании по распространению вредоносного ПО, связанные со шпионажем, начиная с 2012 года. Эта группа часто соответствовала целям китайской коммунистической партии, изложенным в 13-й пятилетней программе «Сделано в Китае 2025».

Известно, что они атаковали компании видеоигровой индустрии, телекоммуникационные компании и научно-образовательные учреждения. И я уже рассказывал в сентябре, что министерство юстиции США предъявило обвинения нескольким лицам, имеющим отношение к атакам и операциям APT41. Следующий слайд, пожалуйста.

Так, недавно исследовательская и разведывательная группа Blackberry разоблачила кампанию по распространению вредоносного ПО, проводимую группировкой APT41 с использованием собственного настраиваемого профиля для сокрытия трафика в сети. APT41 также использует различные вредоносные программы, такие как PlugX, Cobalt Strike, [невнятно], ShadowPad. Также была раскрыта инфраструктура APT41 путем захвата некоторых совпадающих индикаторов компрометации, связанных с двумя кампаниями, зафиксированными двумя другими охранными фирмами, Positive Technologies и [невнятно]. Как видно из доменов, они пытались маскироваться под легитимные домены Microsoft. Это касается первых трех, последних трех, пяти или шести доменов. Следующий слайд, пожалуйста.

Итак, инструмент поиска регистрационных данных ICANN позволяет выполнять поиск доменных имен и ресурсов нумерации интернета по набору текущих регистрационных данных. Чтобы провести это исследование, пользователям потребуется зайти на сайт WHOIS.icann.org и ввести любой домен. В частности, я выбрал

isbigfish.xyz, и когда ввел домен, вот какая информация была получена.

Таким образом, поиск этих доменов и IP в различных хранилищах разведки по открытым источникам выявил некоторые связи, требующие дальнейшей проверки. Упомянутый здесь домен принадлежит IP-адресу 107.182.24.93, который фигурирует в блоге кампании по распространению вредоносного ПО от Positive Technologies. Таким образом, они смогли соединить точки, используя эти открытые источники и обнаружив некоторые из этих IP-адресов, доменов, и что они используют для получения доступа к различным инфраструктурам и сетям.

По датам сертификатов видно, что они действуют только около года, а это своего рода тревожный сигнал с точки зрения практического специалиста, поскольку обычно субъекты, создающие угрозы, используют такие поддельные или запаркованные домены для некоторых видов вредоносной деятельности. Так что это даст нам много информации. Следующий слайд, пожалуйста.

В заключение скажу, что компании Blackberry удалось найти эту информацию путем сопоставления различных блогов различных специалистов и охранных фирм, которые уже были в открытом доступе. В подобных сценариях мы действительно поддерживаем открытый обмен информацией для создания общей картины и полного представления об угрозе или субъектах, создающих

угрозы. Таким образом, совместными усилиями мы можем раскрывать некоторые виды преступной деятельности, которая ведется в настоящее время. Если у вас есть вопросы, дайте мне знать. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Скотт. У нас есть вопросы? Хорошо, спасибо. Хорошо поработали. И у нас последний на сегодня наш докладчик, Джеймс Пэк (James Paek). Джеймс, прошу вас. Спасибо.

ДЖЕЙМС ПЭК: Большое спасибо, Дебора. Меня зовут Джеймс Пэк, моя тема — цифровой авторитаризм, как ему противостоять. Следующий слайд, пожалуйста.

Довольно многие из вас зададутся вопросом, что же такое цифровой авторитаризм? Исходя из определения, которое было дано, под ним подразумевается использование интернета и связанных с ним цифровых технологий лидерами с авторитарными тенденциями для снижения доверия к общественным институтам, усиления социального и политического контроля и подрыва гражданских свобод. То есть все, что может представлять собой вторжение в частную жизнь, посягательство на общественную свободу и все те вещи, которые мы принимаем как должное, не осознавая, что правительство

может контролировать вас по каждому из аспектов [основы] общества, которые вы можете себе представить.

Я думаю, многое связано с тем, каковы причины цифрового авторитаризма. Это может быть авторитарное правительство, будь то политическая, социальная, экономическая нестабильность, подрыв общественного доверия к институту, повышение легитимности и автономии, контроль и манипулирование общественным мнением. Я думаю, все это объединяет страх. Определенно, мы наблюдаем растущий общественный страх перед тем, что ждет наше общество в будущем, о котором мы не имеем ни малейшего представления, здесь много неопределенности. Конечно, пандемия и все эти вещи, которые происходят прямо сейчас, являются одной из общих причин, по которым, на мой взгляд, мы наблюдаем растущее, усиливающееся общественное недоверие.

И конечно, сюда относится недовольство, и я думаю, что мы имеем слишком много прав и не понимаем, откуда что происходит. И конечно, я думаю, что это очень распространено, национализм, популизм, множество политических организаций начинают оказывать влияние, почему цифровой авторитаризм сейчас и становится нормой во всех странах. Следующий слайд, пожалуйста.

Поэтому я думаю, мы начинаем видеть много тенденций в этом вопросе. Возьмем, к примеру, Китай, где в последнее время

определенно все больше видеонаблюдения, камеры в китайских городах установлены на каждом углу. Повсюду, в каждом секторе, на каждому углу улицы, по которой вы идете. Определенно, на каждом участке вы видите множество камер видеонаблюдения, которые потенциально [могут оценивать] любой проступок, будь то агрессивное вождение, некорректное поведение в обществе или что угодно, что потенциально может быть расценено как буйное поведение. И это те вещи, которые мы сейчас часто встречаем, и это определенно так. Мы видели это в Гонконге, где правительство Китая начинает усмирять [граждан Гонконга]. Мы видели это в связи с законопроектом об экстрадиции в 2019 году, с недавним принятием Китаем закона о национальной безопасности. Не буду вдаваться в подробности, скажу лишь, что недавнее сдерживание сопротивления в Китае восходит к тому, что мы видели во время культурной революции 1950-х годов или в эпоху холодной войны. Мы начинаем видеть, как это во многом проявляется в Китае. Может ли такое случиться в других странах? Определенно может. Мы просто не знаем, что произойдет... и определенно начинаем видеть действие системы социального рейтинга.

Остановимся на этом подробнее. Что представляет собой система социального рейтинга? Это национальная система доверия, основанная на оценках вашего общественного поведения. Как я уже говорил, это может быть агрессивное вождение, плохое поведение или любой ваш поступок, который Коммунистическая

партия Китая может отнести к ненадлежащему общественному поведению. На основании этих рейтингов вас могут наказать по любой причине, и потенциально вы потеряете много привилегий, таких как право выезда в другие страны. Или понесете какое-то наказание.

Конечно, мы видели, как это происходило ранее в Южной Корее, когда национальная разведывательная служба начала составлять «черные списки» корейских деятелей культуры в связи с их политическими взглядами. И ведение психологической войны предыдущим правительством в прошлые годы, и запугивание пользователей Интернета. И безусловно, мы наблюдаем значительное усиление слежки и цензуры в отношении тех, кто ведет антигосударственную деятельность, что бы они ни относили к выступлениям против политики правительства. Следующий слайд, пожалуйста.

В других странах тоже, что мы видим сейчас в России, Беларуси и Франции, все чаще это усиление слежки и цензуры. С подтасовкой результатов выборов Александром Лукашенко в Беларуси и недавним отключением интернета. Мы видим вмешательство в выборы в России и очевидное вмешательство в выборы в других странах. Это постоянно происходит в других странах, где мы видели много фальсификаций на выборах, и я думаю, это действительно большая проблема доверия к выборам и самих выборов и системы голосования. И это потенциально может повлиять на многие социальные модели поведения путем ведения

пропаганды. И мы видим, что то же самое происходит во Франции, где, по сути, закон о национальной безопасности даст французскому правительству широкие полномочия по наблюдению за любым человеком, с учетом масштабов агрессии в отношении правоохранительных органов, и преследованию граждан, нарушающих закон. Следующий слайд, пожалуйста.

Цифровой авторитаризм может реализоваться множеством различных способов. Несомненно, я уже упомянул слежку, цензуру. Сюда же относятся махинации на выборах, полицейский произвол, дезинформация, распространение ложных сведений, а также цензура. И в дополнение к этому следующий слайд. Следующий слайд, пожалуйста.

И, конечно, их очень много. Распознавание лиц, кибератаки и хакерство. Многое из этого фактически считается цифровым авторитаризмом, о котором мы никогда не думаем, но все это относится к цифровому авторитаризму, включая шпионаж, фейковые новости и информационные цифровые фабрикации, которые, по сути, представляют собой манипуляцию на основе оригинальной фотографии или видео и попыткой манипуляции в другом формате. Сейчас это до такой степени распространенное явление, что многие граждане и рядовые пользователи интернета не могут определить, оригинальный это источник или нет, и потенциально это оказывает большое влияние на повседневную общественную жизнь, на то, как мы ее интерпретируем. Следующий слайд, пожалуйста.

Чем угрожает рост цифрового авторитаризма? В широком смысле это подрывает демократию, включая институт, а также потенциально может подорвать [во многом социально-экономическую, политическую сферу] и саму культуру, и в то же время является нарушением прав человека и гражданских свобод. И еще... это случается нечасто, но потенциально это также может повлиять на права женщин, в том числе на рост сексуальных домогательств или на причинение другого вреда человечеству. Следующий слайд, пожалуйста.

В том числе с этим может быть связано все здесь перечисленное, а также другие угрозы. И я уже упоминал, что все эти угрозы цифрового авторитаризма могут иметь нежелательные последствия в ближайшем будущем. Следующий слайд, пожалуйста.

Если взглянуть на последние данные, основанные демократическом индексе от «Economist Intelligence Unit», по демократии, мы увидим, что сейчас мы находимся в состоянии пандемии, и многие страны и правительства по всему миру начинают использовать множество инструментов и множество оправданий тому, как мы могли бы на самом деле действовать и в принципе действовать в будущем, как противостоять пандемии, включая пути восстановления демократических институтов и общественного порядка.

И мы видим, что в нашей стране, США, почти начинают появляться гибридные режимы, или, что очевидно в данном случае, у нас сейчас слабая демократия. Изначально мы постоянно выигрывали за счет полной демократии, но, к сожалению, у нас начинаются ухудшения, обусловленные последними событиями, в основном на выборах и во всем, что сейчас происходит. Но если посмотреть на другую часть мира, там практически то же самое. Во многих странах имеет место ослабление демократии, и это вызывает тревогу и опасения, что если мы не сделаем ничего, чтобы противостоять этому цифровому авторитаризму, и позволим правительствам действовать по принципу аврала, чтобы они и дальше использовали многие из этих инструментов в нашей повседневной жизни, это нанесет вред нашему обществу, тоталитаризм нам не нужен... Северная Корея или Китай, как мы видим, они собираются экспортировать большое количество этих средств, камер наблюдения, что бы это ни было, и мы должны положить этому конец. Следующий слайд, пожалуйста.

И вы спросите себя, как противостоять этому, как найти решение. Есть много способов, разных методов. Но я бы сказал, самое главное, что мы должны сделать, это продвигать демократию, права человека у себя дома. Это первоочередная задача.

Я хотел бы, чтобы США подавали пример. Если мы не справимся с внутренними проблемами, то мы не сможем подать пример всему остальному миру и, по сути, принудить другие страны и сказать: «Вы должны соблюдать наши права», по сути, вы должны

поддерживать права человека и убедиться, что у каждого есть право на свободу, чтобы поддерживать все эти свободы.

Но, к сожалению, если США не могут сделать это у себя дома и, по сути, не хотят преодолеть эти [невнятно] проблемы, то, к сожалению, нет оснований, по которым они могли бы стать примером для других стран по всему миру. По аналогии я бы сказал, если вы выполняете дипломатическую миссию и представляете США или другие страны, то люди будут оценивать и воспринимать вас с учетом вашего характера или того, какой вы человек. Здесь может быть то же самое. Поэтому нам необходимо повысить доверие к государственным институтам, включая правительства.

Для этого необходимо убедиться, что мы укрепляем [культуру], чтобы предотвратить политическое и социальное [недоверие]. Сюда относится ослабление межрасовой напряженности, которая присутствует у нас в США, и предотвращение раскола страны. Это одна из самых больших проблем, которая мне очень не нравится, и определенно, нам нужно это исправить, чтобы обеспечить единение. Понимаю, что реализовать это, безусловно, труднее всего, но мы должны укреплять цивилизованность, чтобы мы представляли хороший социальный характер и поведение, чтобы в том числе, США укрепляли свободу интернета, цифровую инклюзивность и доступность. Следующий слайд, пожалуйста.

Это включает в себя целый ряд вещей. В основном, укрепление многосторонних коалиций, что мы видим в последнее время с США [неразборчиво] диалог по безопасности альянса QUAD, включая «пять глаз», укрепление этого альянса. И есть вероятность, что в будущем мы можем столкнуться с азиатским НАТО. Мы пока не знаем, но [этот тренд, этот потенциал] мы видим уже сейчас.

И много государственных инвестиций. Определенно, нам нужно инвестировать в человеческий капитал. Я знаю, что Китай, безусловно, потенциально наращивает инвестиции в человеческий капитал, увеличивая число специалистов по кибербезопасности, чтобы и дальше расширять кадровый потенциал. Но у нас в США большой дефицит специалистов по кибербезопасности. И если у нас этого не будет или начнется нехватка кадров в области науки, технологий, инженерии, математики, мы сильно отстанем и можем столкнуться с нежелательными последствиями. Сюда относятся инвестиции в исследования и разработки. Если в них не вкладывать средства, то они точно останутся далеко позади. Сюда относится и множество цифровых технологий, усиление шифрования.

На работе, безусловно, нам нужно усиливать многообразие и инклюзивность на рабочем месте. Безусловно, корпорация [должна двигаться вперед] и идти в будущее, планировать, чтобы нанимать лучших специалистов, в том числе обеспечивать устойчивость в условиях любого национального кризиса, такого как, например, пандемия, в которой мы сейчас находимся, и

многое другое, что мы должны сделать, чтобы и дальше удерживать позиции лидера в области технологий. Следующий слайд, пожалуйста.

Это ссылки и цитаты. Следующий слайд, пожалуйста. Это конец моих слайдов. Благодарю вас за то, что вы послушали мою презентацию на тему этих глобальных трендов и уделили мне время. Большое спасибо. А сейчас я готов ответить на ваши вопросы.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Джеймс. В чате есть вопрос от Брайана. В принципе, он был адресован, я думаю, всем, но поскольку вы выступали, то спросим вас. Что вы думаете о свободе слова в интернете во время COVID-19?

ДЖЕЙМС ПЭК: Спасибо за этот вопрос, Брайан. Я не совсем понимаю, о чем вы пытаетесь спросить. Уточните, если можно.

ДЕБОРА ЭСКАЛЕРА: Брайан, вы можете уточнить?

ДЖЕЙМС ПЭК: Мне подождать или просто высказать собственное мнение по этому поводу?

ДЕБОРА ЭСКАЛЕРА: Давайте вы дадите собственную интерпретацию ответа на его вопрос.

ДЖЕЙМС ПЭК: Я думаю, Брайан, это может означать много разных вещей в зависимости от интерпретации [на которую я могу сослаться]. Но если вы думаете о том, что такое свобода слова в интернете во время COVID-19, то, как я говорил в самой презентации, цифровой авторитаризм растет. И многие случаи, которые я представил, Китай, Россия, Беларусь, и многие из этих вещей... не поймите меня неправильно, не ожидайте, что в США полная свобода в интернете и все такое. Определенно, это неправда, потому что нам еще многое предстоит. И в принципе, мы видели, что происходило в 2014 году с Эдвардом Сноуденом, определенно, это был пример того, как правительство собирало огромное количество данных в целях общественной безопасности и обеспечения национальной безопасности после того, что было в мире после 11 сентября.

В настоящее время, как я уже упоминал, мы начинаем наблюдать усиление авторитарного поведения, контролирующего наше общество, и свобода в интернета начинает ухудшаться с учетом всего многообразия инструментов и методов, которые мы видели... например, если вы видели в Африке, в Нигерии, где недавно отключили интернет, включая другие регионы...я точно не знаю, какие еще африканские регионы были затронуты.

Определенно, это нужно в основном для того, чтобы правительство не имело возможности контролировать любой вид свободы информации в интернете, потому что это может привести к серьезным последствиям. Если правительство начинает вас контролировать на основании вашего поведения, любых алгоритмических данных, которые есть в его распоряжении, которые могут воспринимать ваше поведение как неуправляемое, то это действительно вызывает беспокойство, и правительство не должно иметь права подслушивать вас и подвергать цензуре на основании того, как вы себя ведете. По сути, это ваша свобода, ваши права, ваши высказывания, и у вас есть право, возможность убедиться, что они остаются за вами и что правительство не должно переступать границы. Это не их дело... они, безусловно, не должны вмешиваться в вашу личную повседневную жизнь.

Как я уже говорил, нам не нужна еще одна эпоха «большого брата», как это было в предыдущие годы, включая то, что мы видим в Северной Корее, и Китай также идет по этому пути. Хотим ли мы видеть это в остальном мире? Я определенно не хочу. По сути, это вторжение в частную жизнь. Свобода слова, гражданские свободы будут ослабляться на основе такого восприятия до такой степени, что это станет неприемлемым.

Мне не нравится то, что многие страны пытаются проявлять авторитарные тенденции, но я думаю, это то, о чем нужно позаботиться, и мы должны сохранить нашу свободу слова и все гражданские свободы, потому что если мы этого не сделаем, если

мы примем все как должное, мы не можем этого допустить, потому что тогда авторитарные режимы будут контролировать мир. Мы не хотим, чтобы это произошло. Мы должны сделать это, убедившись, что мы инвестируем в себя, и нам необходимо повысить уровень образования, повысить доверие общества к институту.

На данном этапе в США и в остальном мире это трудная задача, но мы обязательно должны активно слушать, в том числе уважать все модели поведения в представлении других людей. Именно поэтому я говорил о повышении уровня цивилизованности, чтобы мы уважали друг друга. И это выходит за рамки самого цифрового авторитаризма, но я думаю, это психологические аспекты того, почему мы должны всегда проявлять уважение, открытость и быть терпимыми к другим, если наши мнения не совпадают. Большое спасибо.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо, Джеймс. Я думаю, Брайан дал уточнение своему вопросу в чате. У нас осталось всего несколько минут, поэтому я его вам зачитаю, но затем попрошу вас ответить очень кратко. Он спрашивает: «Вы упомянули, что правительство контролирует свободу слова в интернете намного строже, чем раньше. Считаете ли вы это положительной тенденцией в демократическом мире?».

Я даю вам всего две минуты, чтобы ответить на это уточнение. Спасибо, Джеймс.

ДЖЕЙМС ПЭК: Как я уже говорил, мы должны инвестировать в человеческий капитал. В основном это означает, что мы должны инвестировать в наших людей, чтобы повышать нашу технологическую грамотность. И если мы этого не сделаем, то столкнемся со множеством нежелательных последствий. Сюда относятся демократические преобразования, и мы должны сначала укрепить демократию у себя, а затем убедиться, что другие страны последуют за нами и тоже установят у себя демократию.

[Не надо сомневаться, что демократия — это, очевидно,] лучшее, что есть в мире. Я не говорю, что она плохая, я просто хочу сказать, что ее определенно нужно укреплять. И это определенно должно быть повышение общественного доверия, чтобы мы доверяли институтам, и достичь этого мы можем, доверившись себе и укрепляя культуру дома. Именно здесь мы должны уважать друг друга.

ДЕБОРА ЭСКАЛЕРА: Хорошо. Спасибо. Похоже, у Инека есть вопрос. Я дам вам одну минуту, чтобы ответить на него, потому что нам пора заканчивать. Инек, ваш вопрос?

ИНЕК НИКИНГБОУНГ ДУУТ: Большое спасибо. Это не вопрос, просто дополнение к заданному вопросу. Я думаю, очень важно обратить внимание на тот факт,

что некоторые правительства действительно воспользовались ситуацией с COVID, чтобы принять законы, дающие им право получать доступ или перехватывать цифровую информацию, которой обмениваются люди, и использовать это в качестве оснований для преследования или предъявления исков, что представляет своего рода более высокую версию модерации контента.

И некоторые из этих законов не стали новостью, потому что все были против дезинформации и распространения ложной информации в период COVID, но действие этих законов запланировано не до завершения периода COVID, поэтому мы можем увидеть, как правительства принимают эти законы, принятые во время COVID, и используют их как преимущество, чтобы препятствовать свободе слова и по завершении периода COVID. Я думаю, это очень важная тема, которую нам, возможно, стоит рассмотреть подробнее. Большое спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо за комментарий. Хорошо, на этом мы завершаем сегодняшнее заседание. Хочу поблагодарить всех за то, что поддержали нас сегодня, за участие. Спасибо Сирануш за работу со слайдами. Спасибо нашим докладчикам за проделанную работу. Вы отлично поработали сегодня, очень хорошо, отличные темы и отличная презентация. Спасибо технической группе за поддержку и нашим переводчикам. Без вас мы бы не справились. И

благодарю всех, кто присутствовал сегодня и поддерживал наших участников NextGen@ICANN 72. Мы очень рады, что вы здесь с нами. И обращаюсь к участникам NextGen: проведите время с пользой на конференции ICANN 72. Мы многое запланировали для вас на этой неделе. Знаю, что аббревиатуры и все остальное запомнить трудно, но просто не торопитесь и получайте удовольствие. И спасибо всем за то, что вы сегодня здесь. Вот и все. Желаю вам отлично провести день.

[КОНЕЦ СТЕНОГРАММЫ]