ICANN74 | Форум по формированию политики — презентации по программе NextGen (1 из 2)
Вторник, 14 июня 2022 года — с 13:15 до 14:30 по AMS

ДЕБОРА ЭСКАЛЕРА (DEBORAH ESCALERA): Здравствуйте и приветствую вас на презентации по программе NextGen на конференции Интернет-корпорации по присвоению имен и номеров (ICANN). Меня зовут Дебора Эскалера, и на этом заседании я исполняю обязанности менеджера удаленного участия.

Пожалуйста, помните о том, что это заседание записывается, и придерживайтесь стандартов ожидаемого поведения ICANN. Во время заседания опубликованные в чате вопросы и комментарии будут зачитываться только в том случае, если они соответствуют установленной форме, как я указала в чате. Я буду зачитывать вопросы и комментарии в указанное председателем или модератором этого заседания время.

На заседании будет выполняться устный перевод на английский, испанский, французский и русский язык. Нажмите кнопку перевода в Zoom и выберите язык, на котором вы хотите слушать это заседание.

Если вы хотите выступить, поднимите руку в виртуальном зале заседаний Zoom, а когда координатор конференции назовет ваше имя, включите свой микрофон и говорите. 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.

А сейчас я хотела бы поприветствовать вас на заседании и поблагодарить участников программы NextGen в ICANN за проделанную работу по подготовке презентаций. Я также хотела бы поблагодарить своих наставников, Софи Хей (Sophie Hey), Дессален Йегуала (Dessalegn Yehuala) и Роберто Гаэтано (Roberto Gaetano), которые работали со студентами в течение последних нескольких недель, координируя их работу в рамках процедуры конференций ICANN. Хочу также поблагодарить свою коллегу Бетси Эндрюс (Betsy Andrews), которая сегодня будет показывать слайды. И теперь я передаю слово нашему первому докладчику Джоэлу Кристофу. Джоэл, прошу вас.

ДЖОЭЛ КРИСТОФ (JOEL CHRISTOPH): Большое спасибо. Всем добрый день, благодарю всех присутствующих лично и онлайн. Я представлю проект «Планирование роста интернета в 2022 году», в котором фиксируются наши источники демографических и экономических знаний и полученная нами из них информация. Следующий слайд, пожалуйста.

Прежде чем начать, я хочу, чтобы все на минуту задумались: какова, по вашему мнению, в странах с низким уровнем доходов доля населения, пользующегося интернетом? Под низким доходом подразумевается дневная прожиточная норма в размере 2,7 евро или меньше.

Второй вопрос: каково, по вашему мнению, в странах с низким уровнем доходов количество подписок на услуги мобильной сотовой связи на 100 человек? Как по вашему, оно ближе к 25, 50, 75, или к какой-то другой цифре?

Наконец: как вы думаете, сколько безопасных интернет-серверов приходится на 1000 человек в Северной Америке? Что касается определения, то это подсчитать будет, возможно, несколько труднее, но я надеюсь, что к концу данной презентации вы сможете ответить на эти вопросы. Следующий слайд, пожалуйста.

В течение последних нескольких десятилетий мы наблюдали изменение предмета исследований и публикаций для множества людей. В числе прочего, мы видели сильный рост интернета в масштабах с 90-х годов и, в более недавней перспективе, в социальных медиа и Facebook. Для сравнения я покажу частоту использования слова «цензура» в литературе, опубликованной на английском языке.

Из этого слайда можно увидеть, что мы всё больше и настойчивее интересуемся многими такими темами. И можно сделать вывод, что исследование этих тем будет оставаться столь же важным и находить отражение в той литературе, с которой нам приходится иметь дело. Следующий слайд, пожалуйста.

Перейдем к основной части вопроса. На этой диаграмме показана доля людей, пользующихся интернетом, по регионам. К сожалению, легенда справа получилась немного кривой. Но суть в том, что во многих регионах мы наблюдаем стабильный рост количества лиц, пользующихся интернетом. В отдельные моменты времени имеет место особое ускорение.

Например, в течение прошедших нескольких лет рост был относительно более быстрым в Юго-Восточной Азии. И имеет место приближение к 90% в некоторых регионах с наиболее

высокими доходами, среди которых первые две позиции, отмеченные синим и красным цветом, приходятся на Северную Америку, а за ними идет Европа и Центральная Азия.

Важно указать на отмеченную коричневым цветом группу с низкими доходами, на которую приходятся страны с наинизшими доходами, согласно категориям Всемирного банка. Опять-таки подразумеваются люди, живущие в среднем на 2,7 евро или меньше в день. И даже в этой группе мы видим, что к интернету имеет доступ почти каждый пятый. Это говорит о том, что доступ к интернету в ряде регионов мира с наинизшим уровнем доходов расширяется по мере диффузии различных технологий, обеспечивающих этот доступ. Следующий слайд, пожалуйста.

Если сравнить эти показатели с абсолютными значениями, то мы видим, что, несмотря на относительно раннее начало пользования в США, отмеченных зеленым цветом, за прошедшее десятилетие имел место значительный рост количества интернет-пользователей в Китае и Индии. Учитывая их относительно большее население, эта тенденция будет и далее отражаться в большом объеме использования. Впоследствии, изменится и количество идей из разных регионов мира.

В нижней части этой цифры довольно много составляющих, но она отражает еще 10 стран из числа 13, занимающих первые места по количеству интернет-пользователей. Примеры: Бразилия, Индия, Российская Федерация. Следующий слайд, пожалуйста.

Теперь сравним количество пользователей с количеством подписок на услуги мобильной сотовой связи, и для этого мы решили лучше разобраться в том, что может представлять собой доверенное лицо, через которое люди получают доступ к интернету. Эти данные переданы через Всемирный банк и основаны на информации Международного союза электросвязи. Как мы видим, во многих регионах, например в Северной Америке, Европе и Центральной Азии, подписок на услуги мобильной сотовой связи гораздо больше, чем людей. Опять-таки в группе с низкими доходами, определенной не географически, а экономически, также приходится как минимум одна подписка на услуги мобильной сотовой связи на двух человек. Это указывает на то, что во всём мире будет расширяться доступ через мобильные сети. Следующий слайд, пожалуйста.

Если сравнить с фиксированным широкополосным доступом, который можно считать альтернативным способом доступа и связи, то налицо менее выраженный

рост. Особенно за прошедшие несколько десятилетий. Мы не видим ни показателя 120 по шкале Y, ни быстрого достижения одной и той же точки разными регионами, особенно в Южной Азии, Черной Африке и экономической категории, определяемой словами «с низкими доходами».

Интересно отметить, что даже среди регионов с наивысшими доходами — возможно, в данном контексте следует рассматривать и Северную Америку — довольно очевидно застревание у порогового значения 50%. Следующий слайд, пожалуйста.

Перейдем к количеству безопасных интернет-серверов на миллион человек. В данном случае подразумевается количество явных TSL/SSL-сертификатов, имеющих общественное доверие и использующих технологии шифрования. Если сравнивать с другими слайдами, то мы видим большую разницу между регионами. В Северной Америке, которая в данном случае представлена прежде всего США и Канадой, очень большой показатель на человека, и далее идет Европа. При этом в большинстве других регионов такие явные сертификаты пока встречаются не очень часто. Следующий слайд, пожалуйста.

Если рассматривать пользование интернетом как долю населения, коррелирующую с ВВП на душу, то можно увидеть

признаки положительной взаимосвязи: чем выше в стране доход на душу населения, тем больше количество пользователей интернета. Но как мы видим в верхнем правом углу графика, существует точка насыщения при показателе около 6000 нынешних международных долларов на душу населения. Это приблизительно соответствует уровню доходов в Норвегии, Бахрейне, США или Швейцарии, а при более высоком уровне доходов дальнейшего роста не происходит, потому что достигнуто насыщение доступом к интернету. Следующий слайд, пожалуйста.

На последнем слайде я хочу подумать вот над чем: когда мы пытаемся изобразить расширение в пространстве и времени, на графике видно не только экстенсивное использование доступа к интернету, но и интенсивное.

Это основано на данных исследований в США. Людей спрашивали о том, сколько часов в день они взаимодействуют с цифровыми медиа. С 2008 года были разработаны новые устройства и технологии, но особого внимания заслуживают мобильные устройства, которые не заменили собой существующие полностью, но увеличили то время, которое люди уделяют взаимодействию с такими медиа.

Из этого можно сделать вывод: разработка новых технологий и новых способов доступа приведет не к полной замене существующих, а к увеличению времени цифрового подключения в нашей жизни.

На этом я завершу свою часть заседания. Благодарю вас и передаю слово Деборе. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Джоэл. У кого-нибудь есть вопросы к Джоэлу? Давайте проверим, есть ли что-то от онлайн-участников. Хорошо, большое вам спасибо за презентацию. Очень хорошая презентация. Ладно, тогда переходим к следующему докладчику, Мирабелле Кнобен. Мирабелла, вам слово.

МИРАБЕЛЛА КНОБЕН (MIRABELLA KNOBEN): Большое спасибо. Приветствую всех. Спасибо за участие в этом заседании. Сегодня я хочу выступить по теме своего доклада на семинаре, который составила прошлым летом. Это вроде кандидатской диссертации. Я участвовала в семинаре, посвященном Закону о цифровых услугах (DSA), о котором вскоре расскажу. Моей темой было регулирование контента посредством алгоритмов, в особенности — принципы,

необходимые для соблюдения прав человека в цифровой сфере. Следующий слайд, пожалуйста. Да, спасибо.

Итак, насчет Закона о цифровых услугах. Как мы все знаем, Facebook, Instagram, Google, WhatsApp и т.д. — это лишь несколько из крупных онлайн-платформ, с которыми мы ежедневно взаимодействуем. Уверена, вы все по собственному опыту знаете, насколько сильно они влияют на наше мнение и насколько важна их роль в обеспечении нас информацией. В декабре 2020 года, чтобы обновить ныне устаревшие положения Директивы об электронной торговле от 2000 года, Европейская комиссия опубликовала проект так называемого «Закона о цифровых услугах».

В нём, по сути, излагаются более строгие правила в отношении так называемых «очень крупных онлайн-платформ», сокращенно — VLOP. Недавно, в конце апреля, было достигнуто политическое согласие в отношении DSA между Европейской комиссией, Европейским советом и Европейским парламентом. Поскольку это положение, а не директива, после принятия DSA будет действовать на всей территории Европейского союза и начнет применяться не позднее 1 января 2024 года. Следующий слайд, пожалуйста.

Итак, как именно в контексте Закона о цифровых услугах выглядят алгоритмы или системы рекомендаций? В DSA они

определяются Статьей 2, буква O. Согласно определению, это полностью или частично автоматизированные системы, предлагающие тот или иной контент пользователю через пользовательский интерфейс. В техническом смысле, цифровые платформы можно рассматривать как системы рекомендаций, поскольку пользователям таких платформ ежедневно показывается подобранный контент, которому присваивается приоритет относительно другого контента. Следующий слайд, пожалуйста.

А теперь перейдем к сути моего выступления, моей презентации на семинаре: что может мешать соблюдению прав человека? Я сосредоточилась на свободе информации и свободе слова — оба эти права заявлены в Хартии по правам человека.

Сперва поговорим о свободе информации. Социальные медиа-платформы созданы для удовлетворения пользователя. Опять-таки, уверена, всем известно, что они рассчитаны на возвращение людей к тому контенту, с которым они согласны или о котором уже знают. Очевидно, что это может привести к односторонней отчетности и к так называемому эффекту «пузыря фильтров». Ведь если видеть только тот контент, который вам нравится, потому что вы с

ним уже согласились, то может сложиться довольно-таки одностороннее видение.

Если исходить из этого, то свобода слова тоже может оказаться в опасности, поскольку люди формируют мнения на основании той информации, которую им дают. А если информация, которую им дают, создается посредством алгоритмов — то есть человек ее не контролирует, — формирование мнений тоже становится подвержено воздействию извне. Поэтому алгоритмы создают опасность и для свободы слова. Следующий слайд, пожалуйста.

Вопрос звучит так: каких принципов нужно придерживаться, чтобы предотвратить такого рода вмешательство? В своем докладе на семинаре я сосредоточилась на двух возможных принципах. Во-первых, это системы, основанные на так называемом «совместном участии». Суть этого термина ясна из названия. Подразумевается, что системы, основанные на совместном участии, предполагают большее участие людей и, как следствие, отражают ценности большего количества людей. Цель в том, чтобы создать алгоритмы, оправданные с моральной точки зрения, работающие с учетом общепринятых ценностей.

Уверена, что все мы слышали, особенно хотя бы раз за последние несколько дней, о модели ICANN с участием

многих заинтересованных сторон, которая, как мне известно, является внутренней моделью ICANN. Но мне кажется, что основной ее замысел можно реализовать и в социальных медиа-платформах. Основная цель модели — дать голосам всех заинтересованных сторон, групп интересов, равные возможности быть услышанными. Как следствие, основной акцент делается на децентрализованном управлении, всеохватности и совместности процедур.

Учитывая масштабы очень крупных онлайн-платформ, таких как Instagram или Facebook, эту модель реализовать довольно трудно. Однако, как я уже сказала, основополагающее стремление дать возможность всем группам интересов быть услышанными — хороший способ улучшить транспарентность и атмосферу онлайн-участия. Что касается транспарентности — следующий слайд, пожалуйста.

В Статье 29 Закона о цифровых услугах заявлены два требования. Первое — улучшение транспарентности. По сути, это означает, что очень крупные онлайн-платформы обязаны раскрывать свои наиболее значимые параметры, чтобы пользователи знали, с какими параметрами они имеют дело в контексте систем рекомендаций.

Во-вторых, так называемая «возможность отказа». Если говорить простыми словами, то это означает, что, открывая приложение Instagram или Facebook, вы получаете два варианта: с системой рекомендаций и без нее. Как именно это реализовать, пока непонятно, но мне кажется, что это может быть что-то вроде того, с чем мы сталкиваемся ежедневно, открывая сайт и соглашаясь на использование файлов cookie.

Замысел состоит в том, чтобы предотвратить несоблюдение права на свободу слова и других основных прав, а также повысить доверие пользователей к онлайн-платформе, что может быть полезно и для самой платформы.

В завершение скажу, что, прежде чем станут понятны основные элементы самой реализации, необходимо сперва привлечь внимание к вопросам основных прав, чтобы повысить актуальность этой темы в целом. Интернет не имеет границ, и, хотя Закон о цифровых услугах и является европейским, я убеждена в необходимости международного решения. Как мы все знаем, интернет не заканчивается на границах ЕС. На мой взгляд, это единственный способ обеспечить безопасность и привлекательность онлайн-мира в долгосрочной перспективе. Спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Мирабелла. Есть ли вопросы к Мирабелле? Давайте посмотрим. Онлайн-участники? Хорошо, большое вам спасибо за вашу презентацию. Теперь мы перейдем к следующему докладчику, Яну Батцнеру. Ян, вам слово.

ЯН БАТЦНЕР (JAN BATZNER): Приветствую всех. Большое спасибо за эту возможность. Безопасность интернета является нашей общей целью. Поэтому давайте сегодня поговорим о кибер-происшествиях. Следующий слайд, пожалуйста.

Кибер-происшествие — это неблагоприятное с точки зрения безопасности событие, которое приводит к утрате конфиденциальности и целостности в том виде, в котором они определены ICANN. В качестве примера можно привести атаку типа «отказ в обслуживании», при которой злоумышленник делает устройство недоступным для предполагаемых пользователей. Или, возможно, более актуальный пример — атака с подменой. Попытка выдать себя за кого-то другого. Например, использование домена Instagram.xyz с целью получения информации, которую вводит пользователь. На один слайд назад, пожалуйста. Хорошо, спасибо.

Сегодня я хочу оценить распространенные варианты открытых источников данных о кибер-происшествиях. Сегодня я хочу рассмотреть вместе с вами источники и базы данных, которые открыто предоставляют информацию о таких кибер-происшествиях, как они ее предоставляют и как ее можно оценить. Перед собой вы видите составленный мной сетевой график. На нём кибер-происшествия сгруппированы по странам, в соответствии с последствиями. Каждая точка соответствует стране, а при помощи цветовой палитры отражается степень напряженности конфликта. Следующий слайд, пожалуйста.

Между этими источниками данных есть различия. Например, в журнале происшествий кибербезопасности ICANN фиксируются все происшествия в сфере кибербезопасности, случающиеся в пространстве и продуктах ICANN. Уязвимость безопасности — это слабое место в продукте, которым могут воспользоваться хакеры. Всё происходящее в продуктах ICANN фиксируется здесь.

Все наборы данных, представленные ниже, получены из пространства общественной политики. В этих открыто предоставляется информация о любого рода актуальных политических кибер-происшествиях. Сегодня я хочу рассмотреть эти наборы данных, как они оценены, и

спросить, какую информацию мы можем из этого извлечь и какие выводы сделать. Следующий слайд, пожалуйста.

Вот так выглядит журнал происшествий кибербезопасности ICANN. Здесь указывается дата, суть происшествия, состояние и имеющаяся информация в виде единого текстового блока в крайней правой части. Чтобы вам было яснее — в данный момент каждое из перечисленных происшествий имеет состояние «закрыто». Следующий слайд, пожалуйста.

А теперь рассмотрим подходы общественной политики. При разборе этих наборов данных нам нужно, чтобы все строки полностью повторялись и показывали абсолютно одно и то же, поскольку, согласно замыслу, они предназначены для измерения одного и того же.

Мы же видим нечто иное. Зеленым цветом выделены сведения Гейдельбергского университета. Желтым цветом выделены данные отслеживания, выполняемого Советом по международным отношениям. Синим цветом выделен набор данных о диадных конфликтах Валериано и Манесса. Все источники показывают разное количество наборов данных в разные моменты времени, из чего следует, что для их сбора использовались очень разные методики. Наиболее всеохватными являются те, которые выделены зеленым

цветом, данные Гейдельбергского университета. Следующий слайд, пожалуйста.

Продолжим обсуждать данные Гейдельбергского университета и зададим вопрос из области политологии. Если сгруппировать их по странам, то можно получить постепенную картину того, сколько кибер-происшествий направлено в ту или иную страну. Можно понять, сколько кибер-происшествий направлено из той или иной страны. И, как следствие, проанализировать взаимность. Если в направлении страны имеет место происшествие в области кибербезопасности, отвечают ли они другим происшествием?

На этом графике показаны десять стран, наиболее склонных к конфликтам. Даже среди них уровень взаимности низкий. Идеальный уровень взаимности равен 1. Отсутствие взаимности — 0. Даже те, которые наиболее склонны к конфликтам, имеют показатель не более 0,5. Следующий слайд, пожалуйста.

Также следует попробовать понять, насколько возможно привести информацию в количественную плоскость. Передо мной режимы, в отношении которых проводились измерения рейтинга Freedom House и различных характеристик конфликтов в области кибер-происшествий.

С левой стороны мы видим соотношение степени исходящих происшествий и рейтинга Freedom House. С правой стороны — отношение взаимности и рейтинга Freedom House. Из этого мы никаких четких выводов сделать не можем. Мы не видим никаких подобных соотношений. Следующий слайд, пожалуйста

Одна из причин заключается в том, что существует несколько взаимоисключающих состояний, которые значительно искажают подобные политологические подходы. На эту тему многое написано, и существует множество подходов с попытками перевода в количественную плоскость, но я хочу отметить, что такие подходы могут быть очень опасны или вводить в заблуждение. Здесь отмечены красным действительно актуальные страны, на которые нам нужно обратить внимание. Следующий слайд, пожалуйста.

Итак, я подведу итоги. Из сказанного можно сделать три основных вывода. Во-первых, целью всех этих подходов является транспарентность. Транспарентность главным образом достигается посредством, например, журналов происшествий, сотрудничества заинтересованных сторон и внимания к вопросам методики. И ранее на графике мы видели, что методика в значительной степени влияет на

ответы, которые могут быть даны на один и тот же вопрос, заданный в рамках исследования. Большое спасибо.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Ян. Есть ли вопросы к Яну? Проверьте, есть ли что-то от онлайн-участников. Хорошо, большое вам спасибо за презентацию. Мы переходим к нашему следующему докладчику, Надежде Артеевой. Надежда, вам слово.

НАДЕЖДА АРТЕЕВА (NADEZHDA ARTEEVA): Приветствую всех. Мне очень приятно находиться здесь с вами. Я начинаю свою презентацию о злоупотреблении системой доменных имен (DNS) в ЕС. Почему оно существует и как его можно побороть.

Основная проблема с определением злоупотребления DNS состоит в том, что постоянно возникают новые его виды, и их частота с течением времени то возрастает, то понижается. Это было отмечено Консультативным комитетом по безопасности и стабильности (SSAC) ICANN в 2021 году. Но существует определение, согласованное ICANN и сторонами, связанными договорными обязательствами, и оно довольно недвусмысленно. Согласно ICANN, под злоупотреблением DNS подразумевается вредоносное ПО, ботнеты, фарминг,

фишинг и спам в тех случаях, когда он используется [для нанесения ущерба].

Зачем нужно определять злоупотребление DNS? Потому что большинству регистраторов и регистратур нужно конкретное определение видов технического ущерба, которое им понятно, дает возможность ответной реакции и ограничивает последствия неточного и зачастую неадекватного подхода.

Поэтому в начале 2022 года Европейская комиссия выпустила ряд публикаций о значимости этой темы для национальных доменов верхнего уровня (ccTLD), например исследование злоупотребления DNS и сообщение о стратегии ЕС в отношении стандартизации. В своей презентации я буду несколько раз ссылаться на исследование злоупотребления DNS, поскольку это, на мой взгляд, один из самых [неразборчиво] документов в рамках стратегии ЕС по [противодействию] злоупотреблению DNS.

Согласно Европейской комиссии, предполагается оценить охват, последствия и масштаб злоупотребления DNS, а также внести предложения на предмет возможных мер в области политики, исходя из [неразборчиво] пробелов. И злоупотребление DNS определяется как любая деятельность, при которой доменные имена или протокол

DNS используются для вредоносных или незаконных действий. Следующий слайд, пожалуйста.

Поговорим немного об истории вопроса злоупотребления DNS — не только в ЕС, но в сообществе ICANN в целом. Некоторые договорные положения, регулирующие злоупотребление DNS, изначально стали результатом работы в области политики, проводимой сообществом ICANN в 2009 и 2010 годах посредством Рабочей группы по борьбе со злоупотреблениями регистрацией. Таким образом удалось дать определение злоупотребления DNS, уже упомянутое мной, и изложить основные элементы стратегии ICANN, которые были развиты в дальнейшем.

Более шести лет назад SSAC в документе SAC077 написал о предлагаемом ICANN индексе состояния рынка — это стало одной из первых попыток борьбы со злоупотреблением DNS. На слайдах вы видите цитаты. Они предложили реализовать некое мероприятие по аудиту с обязательным раскрытием в будущем аспектов деятельности и поведения регистратур и регистраторов таким образом, чтобы сделать акцент на защите потребителей, а не на отраслевых нормах.

Согласно некоторым сторонам, в течение последующих лет было сделано немного, либо недостаточно. И данная проблема стала особо актуальной ввиду пандемии COVID,

поскольку, согласно большинству оценок, объем регистраций новых доменов, включающих слова «коронавирус» или «COVID», в 2020 году вплотную следовал за распространением этого смертоносного вируса.

Примерно в это время была сформирована Коалиция по борьбе с киберугрозами, связанными с [COVID-19], которая представляла собой группу из нескольких [неразборчиво] экспертов в сфере безопасности, и они опубликовали данные, исходя из которых, можно заметить увеличение количества доменов в последнюю неделю февраля. Примерно в это же время Центры по контролю и профилактике заболеваний США начали открыто предупреждать о вероятной неизбежности серьезной глобальной пандемии.

Изначально ICANN призывала регистраторов в феврале быть более проактивными. Конкретные механизмы при этом не рекомендовались. Однако внимание правительства привлекло злоупотребление DNS, связанное с COVID. Например, несколько [неразборчиво] отправили открытое письмо главам компаний, занимающихся доменными именами. В целом оно привлекло внимание правительств по причине негативных последствий для борьбы с пандемией, о которых в нём говорилось.

Поэтому в мае 2020 года ICANN усилила меры по [неразборчиво] проблемой, был разработан и опубликован для общественности подробный алгоритм [неразборчиво], где излагалась стратегия, которой должны придерживаться регистратуры и регистраторы при определении вредоносных доменных имен. Хорошо, следующий слайд, пожалуйста.

Но давайте теперь поговорим о том, почему злоупотребление DNS существует, каковы условия и потенциальная среда его возникновения. В 2021 году было проведено исследование, которое позднее цитировалось и подтверждалось в отчете ЕС о злоупотреблении DNS, который я уже упоминала. В этом исследовании подтверждается, что одной из основных причин возможности злоупотребления DNS является отсутствие контактных данных ввиду Общих положений о защите данных (GDPR).

Как нам известно, Общие положения Европейского союза о защите данных, принятые в мае 2018 года, ограничили публикацию в WHOIS персональных данных, делающих возможной идентификацию. В ответ на это ICANN приняла новую политику, позволяющую регистраторам и операторам регистратур вымарывать или не раскрывать в WHOIS

персональные данные, делающие возможной идентификацию. Согласно некоторым исследованиям, это привело, например, к тому, что теперь 85% владельцев доменов общего пользования верхнего уровня (gTLD) нельзя идентифицировать, и к другим последствиям — цифры вы видите на слайде.

Еще одна проблема, связанная со злоупотреблением DNS — долгий срок жизни сообщения о злоупотреблении DNS. Согласно некоторым недавним исследованиям, средний срок жизни составляет 32 дня. Конечно, это спорное утверждение, и многие регистраторы заявляют о том, что работа с сообщением о злоупотреблении DNS занимает у них до 10 дней или меньше. Но продолжительность этого периода может меняться от случая к случаю. И у некоторых регистраторов он может быть особо продолжительным.

Еще одна проблема, мешающая нам противодействовать и бороться со злоупотреблением DNS — отсутствие знаний о злоупотреблении DNS и о необходимых действиях в случае его обнаружения. Следующий слайд, пожалуйста.

Так как же можно бороться со злоупотреблением DNS в ЕС? В отчете излагается несколько шагов, несколько мер, которые, по мнению авторов, можно принять в ЕС для решения данной проблемы.

Прежде всего, мы имеем рекомендацию выбирать провайдеров с большим количеством стандартов проверки в отношении регистраций доменов. В отчете предлагается соблюдать в отношении регистраторов доменов более высокие стандарты, и они должны осуществлять такую проверку клиентов, при которой подтверждается личность клиента и отсутствие злоупотребления DNS.

Еще один элемент — инициирование решений по предотвращению и исправлению ситуации. Согласно отчету, бесплатный хостинг и поддомены являются теми услугами, которые изначально предполагались как легитимные. Однако сейчас они зачастую используются для осуществления фишинговых атак. Согласно отчету, компаниям следует заниматься проактивным обнаружением подозрительных доменных имен, содержащих ключевые слова, соответствующие целевому бренду.

Еще авторы предлагают усилить принятие механизмов контроля. Зачастую расширения безопасности системы доменных имен могут служить для [аутентификации] связи между DNS-серверами. Однако низкий уровень принятия и недостаток развертывания может привести к тому, что хакеры получат контроль над сеансом просмотра в интернете и перенаправят пользователей на

мошеннические сайты. Поэтому авторы предлагают постоянное принятие протокола идентификации сообщений, создания отчетов и определения соответствия по доменному имени (DMARC) в качестве первой линии защиты на случай компрометации рабочей электронной почты.

Последний элемент — улучшение стандартов для доменов верхнего уровня (TLD). TLD, как мы знаем, является последним компонентом доменного имени. И, к сожалению, TLD общего пользования — это домены, которые наиболее часто становятся объектом злоупотребления. Но некоторые новые gTLD и ccTLD имеют особо высокую концентрацию мошенничества, поскольку на сегодняшний день очень легко получить TLD менее чем за доллар, и фишеры обожают такой легкий доступ. В отчете говорится о том, что для решения этой проблемы нужно принять какие-то меры.

Спасибо. Буду рада ответить на любые ваши вопросы если они у вас есть.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Надежда. Есть какие-либо вопросы? Похоже, у нас вопрос от аудитории. Хотите подойти к микрофону? Спасибо.

[ДЭВИД:] Здравствуйте, я Дэвид [неразборчиво], что-то про ICANN. Здравствуйте. Спасибо за презентацию. Всем спасибо. Мне хотелось бы понять, просите ли вы ICANN делать больше, чем она уже делает. Учитывая всю трудность и спорность вопроса конфиденциальности данных и различных директив, которые могут возникнуть в результате политики ЕС, таких как, например, Уточненная редакция Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем (NIS2) — по-моему, эта директива называлась NIS2.

Возможно, вы могли бы немного рассказать о том, чем, будь по-вашему, ICANN должна сейчас заниматься. Например, вы могли бы сесть с Йораном и сказать: по-моему, вам нужно заниматься вот этим, чтобы снизить уровень злоупотребления DNS. О чём бы вы его попросили и какова, по вашему мнению, вероятность таких действий?

НАДЕЖДА АРТЕЕВА: Понятно, спасибо за вопрос. Высказывания об ICANN в рамках отзыва касались в большей степени конкретно ситуации с COVID. Наверное, когда возникает кризисная ситуация — а они возникают довольно часто, — реакция

должна быть более быстрой. Конечно, в случае со злоупотреблением DNS во время пандемии сами последствия такого злоупотребления были ужасающими, поскольку оно могло стоить людям жизни. И, конечно, это может привести к тому, что люди получат доступ к неверной информации, и к другим негативным результатам. По моему мнению, в данном случае критика в адрес ICANN со стороны некоторых авторов касалась прежде всего способа реагирования ICANN на кризисную ситуацию.

ДЕБОРА ЭСКАЛЕРА: Хорошо, спасибо. Похоже, у нас онлайн-вопрос от Дэвида [неразборчиво]. А, это были вы. Хорошо, спасибо. Хорошо, спасибо, Дэвид. Итак, посмотрим. Можете подойти к микрофону? Спасибо.

МУЖСКОЙ ГОЛОС: Спасибо. [неразборчиво] кое-какая информация о расширениях gTLD, которые наиболее часто становятся объектом злоупотребления. Вы упоминали, что в основном это касается новых. Но ведь есть, как мы знаем, бесплатные, есть более старые, еще ccTLD, которые предлагают бесплатные доменные имена. Вы ответили на вопрос?

ДЕБОРА ЭСКАЛЕРА: Вы можете это повторить? Вас было не очень хорошо слышно.

МУЖСКОЙ ГОЛОС: Да. У вас есть данные тех gTLD, которые наиболее вовлечены в процессы злоупотребления DNS?

НАДЕЖДА АРТЕЕВА: Конечно, в отчетах... спасибо за ваш вопрос. В отчетах информация была представлена кратко, поэтому примеров не было. Если нужно, я могу их найти. Да, могу.

МУЖСКОЙ ГОЛОС: Да, прямо у вас…было очень интересно послушать, и вы отдельно сказали о том, что данная проблема особо касается новых gTLD. Подозреваю, что один из них — .xyz. Что ж, почему бы не назвать их по именам? Возможно, вы могли бы сформировать свой отчет на основе каких-то данных. И вы могли бы поделиться какой-то частью этих данных, если не трудно. Вот и все. Если нет, хорошо.

НАДЕЖДА АРТЕЕВА: Если нужно, то цитируемый мной отчет — это отчет ЕС о злоупотреблении DNS. Поэтому, если нужно, я могу дать на него ссылку или отправить PDF-документы, и тогда вы

сможете сами всё прочитать. Информация находится в разделе рекомендаций по политике, этот раздел — в конце отчета.

ДЕБОРА ЭСКАЛЕРА: Хорошо, большое спасибо. Имейте в виду, что все эти презентации после сегодняшнего заседания будут опубликованы на архивном сайте ICANN. Хорошо, наш последний докладчик — Любомир Никифоров. Любомир, вам слово.

ЛЮБОМИР НИКИФОРОВ (LIUBOMIR NIKIFOROV): Ну, я не привык выступать с презентациями. Спасибо. Следующий слайд, пожалуйста. Следующий слайд. Меня зовут Любо. Любомир Никифоров. Я учусь в Барселонском университете на степень доктора философии, и мои исследования посвящены вопросам информированного согласия, транспарентности и управления интернетом.

Цель сегодняшней презентации — обратить внимание на отсутствие четких указаний насчет информированного согласия в Соглашении между регистратурами и регистраторами. Нынешняя ситуация создает риски в области транспарентности и достоверности для ICANN и ее

заинтересованных сторон. И в конце я привожу несколько возможных решений. Следующий слайд, пожалуйста.

Нынешняя процедура регистрации доменных имен общего пользования верхнего уровня — это договорная процедура с участием трех сторон. Эти три стороны: регистратор, занимающийся обработкой регистрации доменного имени. Владелец домена — лицо или организация, желающая зарегистрировать доменное имя. И оператор регистратуры — организация, обслуживающая регистратуру доменных имен, зарегистрированных в том или ином домене верхнего уровня.

Такое соглашение содержит одну статью. Статей там больше, но одна мне представляется интересной. Статья 2, пункт 18, где устанавливаются требования о защите данных. В той же статье содержится определение персональных данных, требование об уведомлении в вопросах данных, а также сведения об идентификации и согласии получателей данных. Следующий слайд, пожалуйста. Следующий слайд.

Хорошо, спасибо. Вот об этой статье я и говорю. Как видите, в базовом соглашении это единственная статься, посвященная персональным данным. И предполагается, что в ней [охвачена] вся актуальная информация, все актуальные положения в отношении персональных данных. Она очень

трудна для чтения и понимания, что создает вопросы о ее смысле и полезности в конечном итоге. Следующий слайд.

В чём состоят проблемы? Их несколько. Но я сосредоточусь на проблемах, связанных с требованием о согласии. В соответствии со Статьей 2, пунктом 18, регистраторы должны получать согласие от каждого владельца домена в домене верхнего уровня на сбор и использование персональных данных. Но в Статье 2, пункте 18, не говорится конкретно, каковы требования насчет состоятельности этого согласия и насчет той формы, которую оно должно иметь.

Чтобы проиллюстрировать данную проблему, я обращусь к GDPR, европейской модели регулирования и защиты данных. На этом примере я покажу, что не так. В соответствии с европейскими положениями, согласие должно быть информированным, конкретным, добровольным, недвусмысленным актом волеизъявления субъекта данных.

Из Статьи 2, пункта 18, Соглашения между регистратурами и регистраторами не понятно, как и когда это согласие должно быть получено. Если оно должно содержать точное и полное описание всех целей обработки данных, то какие средства можно использовать? Возможно, допустимо использовать насилие и запугивание? И должна ли информация,

предоставляемая владельцу домена, быть ему понятна. Мы понятия не имеем, может ли владелец домена отказаться давать согласие и какие существуют альтернативы, если отказывается. Следующий слайд, пожалуйста.

Но почему это в конечном итоге важно? Ну, потому что наше общество управляется данными, и информация и данные в нём являются предметом для обмена. Поэтому важно обеспечивать большее доверие заинтересованных сторон и надежность ICANN, а также обеспечивать надежность и доверие к открытому и транспарентному интернету.

Тогда как в ЕС мы можем рассчитывать на конкретные меры защиты в отношении обработки данных, ICANN работает на уровне мировом, глобальном. И нынешние соглашения могут привести к чрезмерному злоупотреблению для владельцев доменов в разных частях света. Процедура, при которой владелец домена понимает цели и ожидаемые результаты обработки данных. И соглашение помогает регистратору, минимизируя возможность непонимания и возможные проблемы с разбирательствами и тяжбами, и создает конкурентное преимущество для регистраторов, а также несет репутационную пользу нашей организации в целом. Следующий слайд.

Как и обещал, я расскажу о возможных решениях. Одно из них, наиболее очевидное, состоит в том, чтобы пересмотреть существующую статью, сделать ее более ясной и легкой для чтения. Возможно, стоит разделить ее на несколько частей. Особенно в случае с согласием. В соответствующих положениях о защите данных должны определяться случаи, в которых необходимо согласие, должно указываться, как и когда согласие следует давать, а также конкретные требования в отношении состоятельности. В качестве примера можно привести GDPR, европейские положения о защите данных, в которых согласие определяется как конкретный, добровольный, информированный и недвусмысленный акт волеизъявления.

Эта модель, конечно, не лишена недостатков. Но если мы можем сохранять свой цифровой отпечаток в качестве продолжения своей личности, то информированное согласие является одной из демократических гарантий нашего цифрового достоинства. Спасибо, и я готов ответить на ваши вопросы.

ДЕБОРА ЭСКАЛЕРА: Спасибо, Любомир. Есть вопросы? Нет вопросов? Давайте проверим онлайн. Хорошо, напоминаю, что все презентации будут опубликованы на сайте ICANN. Если у вас есть другие

вопросы, или появятся позже, то вы всегда можете отправить их мне по электронной почте: engagement@icann.org.

Я благодарю всех за сегодняшнее участие и напоминаю, что второй комплекс презентаций пройдет завтра. Приглашаю вас присоединиться. Огромное спасибо.

[КОНЕЦ СТЕНОГРАММЫ]