ICANN84 | Ежегодное общее собрание – Совместное заседание: GAC и SSAC
Вторник, 28 октября 2025 года – с 15:00 до 16:00 IST (по ирландскому стандартному времени)

GULTEN TEPE [ГУЛЬТЕН ТЕПЕ]: Добро пожаловать на совещание GAC с SSAC, которое проходит во вторник, 28 октября, в 15:00 по универсальному координированному времени.

Обратите внимание, что эта сессия записывается и регулируется Стандартами ожидаемого поведения ICANN, Кодексом поведения участников сообщества ICANN и Политикой противодействия домогательствам в сообществе ICANN. Во время сессии вопросы и комментарии будут зачитываться вслух только в том случае, если они поданы в установленной форме в чате Zoom.

Перевод этого совещания осуществляется на все шесть языков ООН и португальский.

Если вы хотите выступить во время сессии, пожалуйста, воспользуйтесь функцией «Поднять руку» в Zoom. Не забудьте назвать свое имя для протокола и указать язык выступления, если вы говорите не на английском. Пожалуйста, говорите с разумной скоростью, чтобы обеспечить точный перевод.

На этом я хочу передать слово Николасу Кабаллеро, председателю GAC. Спасибо.

NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]: Спасибо большое, Гультен. Добро пожаловать обратно. Очень надеюсь, что вы насладились фантастическим ирландским кофе. Я рад представить нашего хорошего друга и его команду — Рама Мохана из SSAC. А также Сюзанну, Маартена и Тару. Добро пожаловать! Нас ждет очень интересная, по крайней мере на мой взгляд, сессия, разделенная на четыре части.

Первая и самая важная, опять же по моему мнению, — «Значение свободного и открытого программного обеспечения (FOSS) в индустрии DNS». Я бы добавил — и не только там, но это уже тема для отдельного обсуждения. Далее — «Влияние коллизии и схожести строк на безопасность и стабильность». Это в какой-то степени неизбежный вопрос на данном этапе. И наконец — «Возможности сотрудничества между SSAC и GAC». После этого я открою сессию для вопросов и ответов.

Опять же добро пожаловать. Сейчас я передам микрофон моему хорошему другу, Раму Мохану. Вам слово.

RAM MOHAN [РАМ МОХАН]: Нико, спасибо. Для нас большая честь снова выступать перед вами здесь, в Дублине, и особенно перед членами GAC. Мы искренне ценим, что вы на протяжении нескольких встреч продолжаете приглашать нас и выделять время для нас в своем насыщенном графике. Со своей стороны мы не только

высоко ценим эти встречи, но и очень тщательно к ним готовимся. Мы стремимся к тому, чтобы предоставляемая информация и наше взаимодействие с вами были не только релевантными, но и практичными — содержали конкретные выводы, которые вы могли бы использовать в своей работе. Это основа нашего подхода.

Без дальнейших предисловий я хотел бы посвятить первую часть нашего выступления теме «Значение свободного и открытого программного обеспечения именно в индустрии DNS». Чтобы представить эту тему и поделиться с вами деталями, я передаю слово моему коллеге Маартену Аертсену, который являлся одним из сопредседателей рабочей группы по данному вопросу. Маартен.

MAARTEN AERTSEN [МААРТЕН АЕРТСЕН]: Спасибо, Рам. Спасибо, Нико. Сегодня я расскажу вам о программном обеспечении. SSAC обычно готовит довольно технические документы. Этот — не такой, и само сообщество ICANN не является его основной аудиторией. Этот документ написан для регуляторов и политиков по всему миру. Так что, полагаю, я обращаюсь по адресу. А если это не вы, то, уверен, у вас есть прекрасные коллеги, занимающиеся вопросами кибербезопасности.

Давайте поговорим о программном обеспечении. Если резюмировать наш доклад в одном предложении: мы считаем, что DNS построена на свободном и открытом программном

обеспечении. Это не защита этой позиции. Мы не утверждаем, что свободное и открытое ПО лучше. Это констатация того, как DNS фактически устроена. Следующий слайд, пожалуйста.

FOSS означает «свободное и открытое программное обеспечение». «Свободное» относится к свободе, как свобода слова, а не к цене, как бесплатное пиво «Гиннесс» после этого выступления. FOSS определяется четырьмя свободами. Использовать — вы можете использовать программное обеспечение для любых целей. Изучать — вы можете изучать, как работает программное обеспечение, включая его исходный код. Распространять — делиться и распространять копии программного обеспечения. И, наконец, изменять — вы можете изменять программное обеспечение под свои нужды и публиковать улучшения.

Эти свободы, закрепленные в лицензии на программное обеспечение, создают принципиально иную экосистему для разработки, распространения и поддержки ПО по сравнению с моделью коммерческого ПО с закрытым исходным кодом. Хотя между свободным и открытым ПО существуют философские различия, в этом докладе используется термин FOSS, охватывающий обе концепции, основанные на четырех свободах. Следующий слайд, пожалуйста.

Модель FOSS имеет иную структуру рисков по сравнению с программным обеспечением, являющимся частной собственностью. Поскольку большая часть свободного и

открытого ПО поддерживается волонтерами, мотивация играет важную роль. Если люди работают над ПО на добровольной основе, они также могут столкнуться с выгоранием. А это приводит к заброшенным проектам.

Другой риск FOSS заключается в отсутствии гарантий и поддержки по умолчанию. Поэтому операторам необходимо брать на себя ответственность: либо сохранять экспертизу разработки внутри организации, используя свои права на изменение ПО для исправления ошибок, либо приобретать контракты на поддержку.

Когда открытым ПО занимаются не волонтеры, а профессиональные организации, возникает проблема «безбилетника», поскольку программное обеспечение находится в свободном доступе. Может сложиться ситуация, когда финансирование полностью отделено от использования, а сопровождающие проект специалисты входят в состав небольших инициатив или организаций, которые оплачивают их труд. Такие модели уязвимы для финансовых потрясений, вызванных новыми регуляторными требованиями. Например, когда существующая модель финансирования оказывается под угрозой.

Эти риски реальны и присущи модели FOSS. Регулирование, не учитывающее эти компромиссы, может усугубить, а не улучшить ситуацию. Следующий слайд, пожалуйста.

Однако у модели есть и сильные стороны. Здесь мы рассматриваем конкретно DNS, в отличие от предыдущего слайда, где речь шла о FOSS в целом. В контексте DNS мы видим такие преимущества, как прозрачность и коллективная безопасность. Академическое и операторское сообщества поддерживают сильную культуру открытой проверки свободного и открытого ПО для DNS, занимаясь этим десятилетиями. Уже в 90-х годах публиковались исследования, посвященные ошибкам в ПО или способам его улучшения. Эти недостатки открыто обсуждаются и исправляются.

Операторы, опрошенные нами в рамках этого исследования (более 100 участников), ценят возможность самостоятельно диагностировать, проверять и исправлять уязвимости благодаря открытой цепочке поставок. Они не зависят от скорости реакции производителя, а могут действовать проактивно.

В DNS многие популярные проекты поддерживаются не волонтерами, а давно существующими стабильными организациями. Они занимаются сопровождением реализаций программного обеспечения более 20 лет. Эта долговечность создает репутацию, вызывающую доверие операторов.

Еще одно преимущество FOSS в DNS — операционная устойчивость за счет разнообразия. Множество реализаций FOSS позволяют операторам использовать разное ПО, снижая

риски единой точки отказа. Это также снижает барьер для организаций, желающих использовать собственную инфраструктуру, предотвращая риски концентрации или, что стало актуальной темой, зависимости от иностранных субъектов. Давайте перейдем к следующему слайду.

Поговорим о безопасности. SSAC уделяет особое внимание безопасности, и очень важно понимать, что именно ее определяет. Безопасность не определяется тем, является ли исходный код открытым или закрытым. Она не определяется тем, являются ли разработчики наемными сотрудниками или волонтерами. Безопасность также не определяется тем, создано ли ПО коммерческой компанией или некоммерческой организацией.

А что определяет безопасность? Это тщательный обзор кода и всестороннее тестирование, отлаженный процесс работы с уязвимостями, а также активная долгосрочная поддержка с устойчивым ресурсным обеспечением.

Цитируя доклад: «Безопасность любого проекта программного обеспечения определяется качеством процессов его разработки и сопровождения, а не доступностью исходного кода».

Нам часто задают вопрос: «Является ли FOSS более или менее безопасным по сравнению с ПО, находящимся в частной собственности?» Ответ: ни то, ни другое. Безопасность

определяется качеством процесса разработки, а не моделью лицензирования.

Проблема для политиков заключается в том, что у FOSS иная структура рисков. Нельзя копировать нормативные акты из мира частной собственности и ожидать, что они будут работать в реальности, где существует FOSS.

В начале я сделал несколько смелых заявлений. Давайте обратимся к данным. Следующий слайд, пожалуйста. Начиная с уровня системы корневых серверов: мы опросили 12 операторов корневых серверов и попытались определить используемое ими программное обеспечение. Мы наблюдаем доминирование свободного и открытого ПО. Как минимум 9 из 12 операторов корневых серверов используют исключительно свободное и открытое ПО. Даже операторы, использующие коммерческое ПО для выполнения этой роли, часто параллельно запускают FOSS для обеспечения разнообразия и резервирования. Ключевой вывод здесь: это не небольшой процент. FOSS составляет подавляющее большинство в системе корневых серверов. Следующий слайд, пожалуйста.

Мы также изучили операторов доменов верхнего уровня. Эти организации предоставляют авторитетные службы DNS. Ключевой вывод: если посмотреть на операторов, обслуживающих наибольшее количество TLD, то 9 из 10 используют FOSS для своей DNS-инфраструктуры.

Для этой аудитории, возможно, более применимой будет ситуация на уровне национальных доменов верхнего уровня. Если рассматривать только страны, мы обнаруживаем, что 20 из 25 операторов используют FOSS. В совокупности операторы ccTLD обслуживают 234 уникальных ccTLD с его помощью, и это только на том уровне, на котором мы рассматривали данные. Так что в реальности это число еще больше.

Речь идет не о небольших или экспериментальных TLD. Это крупные поставщики услуг, ответственные за миллионы доменов. Несколько примеров: Nominet в Великобритании использует FOSS, CNNIC в Китае использует FOSS — и это лишь некоторые из них. Следующий слайд, пожалуйста.

Рассмотрим системы реестров — базы данных, в которых хранятся домены в пределах TLD. Мы видим две модели. Первая — полностью FOSS-система. Такие существуют. Они не составляют большинства, но их наличие доказывает, что модель жизнеспособна, и это важный момент.

Наиболее популярная модель — это частные системы реестров. Но даже здесь мы обнаруживаем, что эти частные системы не создаются с нуля. Вместо этого они представляют собой коммерческие интеграции, построенные на основе свободного и открытого ПО. И из десяти основных платформ, которые мы изучили, все включают FOSS-компоненты. Таким образом, даже когда бизнес-логика верхнего уровня является

коммерческой, ее основой служит FOSS. Следующий слайд, пожалуйста.

Экосистему резолверов измерить сложнее всего, но и здесь мы вновь обнаруживаем существенное использование, существенное присутствие свободного и открытого ПО. Восемьдесят процентов пользователей по всему миру используют локальный резолвер, и здесь доминирует FOSS. Даже если взглянуть на коммерческие решения, коих существует множество, в большинстве случаев, если заглянуть внутрь того, что они продают, это FOSS. То же самое относится и к публичным резолверам. Ряд из них являются FOSS.

Мы подготовили небольшой кейс в отчете о Cloudflare, у которых коммерческое ядро окружено FOSS. Как минимум четыре крупнейших гиперскалера используют FOSS для своих DNS-решений. Другие используют FOSS-библиотеки в качестве компонентов внутри частных резолверов. Следующий слайд, пожалуйста.

Цитируя отчет: «В наиболее критических частях инфраструктуры DNS FOSS является нормой, а частное программное обеспечение — исключением». Это не преувеличение. Это не защита этой позиции. Это всего лишь строгий вывод из проведенного нами исследования. Ключевые системы именования в Интернете работают в основном на программном обеспечении, которое

разрабатывается совместно и распространяется свободно. Следующий слайд, пожалуйста.

Традиционный регуляторный подход к цепочкам поставок требует соблюдения стандартов безопасности, возможно, путем их возложения на операторов критической инфраструктуры. Вы возлагаете на них ответственность за сбои, а они, в свою очередь, обращаются к своим поставщикам и устанавливают эти требования через контракты. И вы обеспечиваете соблюдение правил через процедуры закупок и доступ на рынок.

Почему это не работает для FOSS? FOSS часто предоставляется для загрузки бесплатно. Может не быть отношений с поставщиком в традиционном понимании. Нет контракта между оператором и производителем, а иногда нет даже самого производителя для регулирования — только волонтер.

Таким образом, возложение бремени за соблюдение требований на операторов с целью воздействия на их цепочку поставок может привести к дестабилизации небольших организаций, поддерживающих это самое ПО. Или, если речь идет о волонтерах, они могут потерять интерес, что приведет к забрасыванию проектов из-за юридических рисков, переходу на частные лицензии или даже уходу от юрисдикции. В результате программное обеспечение, от которого все зависят, становится менее доступным и менее безопасным. Следующий слайд, пожалуйста.

Мы включили в отчет примеры из практики, поскольку крупные юрисдикции, такие как США, Великобритания и ЕС, разрабатывают политики с учетом особенностей FOSS. Я не буду вдаваться в подробности, если нет интереса, но это возможно. Следующий слайд, пожалуйста.

Вот пять практических рекомендаций, которые мы разработали. SSAC нейтрален в вопросе необходимости регулирования. Также не в нашей компетенции высказывать оценочные суждения. Но если в вашей юрисдикции рассматривается введение нормативных актов, пожалуйста, учитывайте ключевую роль FOSS. Признайте, что глобальная инфраструктура зависит от него, и это преимущество, которое следует сохранять.

Консультируйтесь с сообществом открытого ПО. Привлекайте сопровождающих, фонды и операторов к разработке политики и избегайте непредвиденных последствий.

Используйте современные примеры, которые мы собрали, и изучайте новые модели.

Стимулируйте устойчивое развитие. Поощряйте, например, вклад в свободное и открытое ПО как инвестиции в общественную инфраструктуру.

И совместно решайте системные риски, существующие во всей сфере программного обеспечения, а не только в FOSS. Финансируйте экосистемные решения для общих

зависимостей вместо возложения бремени на отдельных сопровождающих.

Думаю, на этом презентацию можно завершить. С нетерпением жду ваших вопросов.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Маартен, за ясную и содержательную презентацию. Как я уже передавал ранее со слов Рама, рекомендую всем перейти по ссылке и прочитать сам отчет.

У нас осталось время на несколько вопросов. Первый в моем списке находится как раз рядом со мной.

NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]: Нет, нет, это Европейская комиссия.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Хорошо, мы начнем сначала с Европейской комиссии. Спасибо.

GEMMA CAROLILLO [ДЖЕММА КАРОЛИЛЬО]: Большое спасибо, господин председатель и заместитель председатель, но я готова уступить слово [неразборчиво], если вы предпочитаете начать с них. Говорит Джемма Каролильо из Европейской Комиссии. Мы относимся к числу

тех, к кому вы обращаетесь, полагаю, учитывая, что три из четырех примеров из практики касаются нас.

Эта тема действительно важна для нас, и я хочу подчеркнуть, что мы как регулятор также извлекли уроки из этого процесса в части того, как учитывать различные характеристики открытого ПО в цифровом регулировании. Это был, я бы сказала, болезненный, но очень полезный процесс, и я думаю, что мы учимся коллективно, и в настоящее время достигаем хороших результатов.

Мой вопрос касается безопасности цепочек поставок, потому что это остается проблемой. Даже если мы пытаемся обойти ее, проблема сохраняется. Есть ли у вас мнение относительно инициатив, таких как реестр компонентов программного обеспечения (software bill of materials), и как это может помочь решить проблему безопасности цепочек поставок? Спасибо.

MAARTEN AERTSEN [MAAPTEH AEPTCEH]: Спасибо, Джемма. Вы спрашиваете, есть ли у SSAC мнение относительно реестра компонентов программного обеспечения. К сожалению, я выступаю от имени SSAC, и мы не рассматривали эту конкретную меру. Я готов высказать свое личное мнение — это мое предварительное предупреждение.

Итак, да, безопасность — это проблема в сфере программного обеспечения — как частного, так и свободного и открытого. Я думаю, что реестр компонентов может помочь в ситуациях,

когда люди или организации покупают частное программное обеспечение, которое внутри в основном состоит из FOSS. Потому что тогда возникают ситуации, когда компонент уязвим, и он уязвим для всех, даже для всех продуктов на рынке. И если вы, как поставщик или даже как покупатель, не знаете, что внутри, то как вы можете начать исправлять положение? В этом смысле, это интересный инструмент. Сейчас еще ранняя стадия его внедрения.

Я высоко ценю ваше замечание об обучении сообща, даже несмотря на то, что сейчас я выражаю личную точку зрения. Мне было чрезвычайно интересно наблюдать за процессом разработки политики в ЕС, и я испытываю удовлетворение от того, что мы смогли включить этот конкретный пример в наше исследование.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Европейская Комиссия, за вопрос. Спасибо, Маартен. В очереди далее Бангладеш, а затем все же председатель рядом со мной. После этого я закрою очередь, и мы, ради экономии времени, двинемся дальше. Итак, Бангладеш, вам слово.

DR. SHAMSUZZOHA [ДОКТОР ШАМСУЗЗОХА]: Спасибо. Говорит Шамсуззоха из Бангладеш. Хочу отметить, что это очень содержательная и комплексная презентация. Особенно для меня, как представителя Бангладеш,

отвечающего за взаимодействие с различными ведомствами по вопросам стандартов безопасности в Бангладеш. Существуют некоторые конкретные [неразборчиво], которые они производят.

Меня особенно заинтересовали два аспекта. Во-первых, мы работаем с [неразборчиво] Бангладеш над установлением их стандартов безопасности и их [неразборчиво]. Что также включает вопросы публикации программного обеспечения, в частности [неразборчиво].

Кроме того, мы отвечаем за взаимодействие с операторами национальной критической инфраструктуры, в частности за внедрение решений типа [CM] и SWOT для обеспечения безопасности операционной деятельности.

И вот в чем заключается наша дискуссия: когда мы пытаемся [неразборчиво] даже в системе государственных закупок, мы продвигаем свободное и открытое программное обеспечение. Но один из аргументов, с которым мы сталкиваемся, касается внутреннего потенциала внутри [неразборчиво], особенно для [неразборчиво], а также проблемы необходимости оперативного [неразборчиво].

Таким образом, если внутренний потенциал в [неразборчиво] отсутствует, возникает серьезный риск, особенно при работе с национальной критической инфраструктурой. И в некоторой степени это касается и операционных затрат.

Поэтому мой вопрос или, скорее, просьба о вашем мнении: как решать эту проблему, особенно когда мы имеем дело с чувствительной критической инфраструктурой? Спасибо.

MAARTEN AERTSEN [MAAPTEH AEPTCEH]: Спасибо. В этом смысле я считаю, что разница между коммерческим ПО и FOSS меньше, чем может показаться. Потому что, если вы управляете критической инфраструктурой, оператор несет ответственность за бесперебойную работу. И если вы решаете использовать FOSS, что большинство и делает, тогда у вас есть либо собственная экспертиза внутри организации, что является затратами. Вам необходимо иметь экспертов. Либо вам нужно найти их в другом месте, и во многих случаях, если вы посмотрите на наиболее популярное программное обеспечение, эти организации финансируются через контракты на поддержку.

Теперь, если бы ситуация была иной и существовало бы только коммерческое программное обеспечение, тогда вы бы платили лицензионные сборы и, предположительно, также получали поддержку. Так что в этом смысле, я думаю, нет такой уж большой разницы, со всеми теми преимуществами, которые мы перечислили в презентации, являющимися различием. Такие как отсутствие привязки к поставщику и т.д.

Однако да, критическая инфраструктура особенная, поскольку имеет требования к времени бесперебойной работы, и для этого необходима экспертиза. Каждый оператор

может делать выбор в зависимости от возможностей, которые предоставляет ему правительство.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Благодарю вас обоих. Мы завершаем и передаём слово Нико, как большому стороннику FOSS.

NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]: Спасибо. Нет, я буду очень краток. Благодарю вас, Маартен, за фантастическую презентацию. Не могли бы вы очень кратко прокомментировать, как открытое ПО помогает правительствам, особенно развивающимся странам, избежать зависимости от поставщиков — не только с точки зрения затрат, но и с точки зрения... Позвольте мне сформулировать иначе: затрат на внутреннюю безопасность.

MAARTEN AERTSEN [МААРТЕН АЕРТСЕН]: Привязка к поставщику — это ситуация, когда вы принимаете решение инвестировать в определенный продукт и затем не можете от него отказаться, потому что сделанные инвестиции слишком велики или затраты на переход слишком высоки.

Преимущество FOSS в ситуации привязки к поставщику, включая вопросы кибербезопасности, заключается в том, что вы не обязаны сохранять отношения с первоначальным сопровождающим. Иногда есть и другие организации,

которые могут поддержать ваше развертывание, включая исправление уязвимостей.

Вы всегда будете зависеть от первоначального разработчика в создании исправлений, но это не так, как в случае с коммерческим ПО, где есть только одна организация, с которой можно работать. Таким образом, я могу представить, что страна с меньшим бюджетом может рассматривать это как стимул для инноваций, пытаясь создать собственную экспертизу на месте вместо того, чтобы платить внешним организациям за пределами страны. Но это, полагаю, выбор, который они могут сделать.

Думаю, это все, что я могу сказать о привязке к поставщику. Это, повторюсь, мое личное мнение, поскольку мы не так подробно освещали этот вопрос в отчете.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Нико, за вопрос, и Маартену — за прекрасный ответ. Учитывая время, давайте перейдем к следующей теме, для обсуждения которой я также пригласил SSAC, отчасти в рамках развития потенциала. В качестве краткого напоминания: я знаю, что в зале присутствует много новых или относительно новых членов GAC, для которых это, вероятно, довольно новая тема. Но она важна и становится еще более значимой по мере приближения следующего

раунда. Итак, поскольку Сюзанна здесь, полагаю, я могу предоставить ей слово по этому вопросу. Спасибо.

SUZANNE WOOLF [СЮЗАНН ВУЛЬФ]: Хорошо, спасибо, Марко. И спасибо, Маартен. Как всегда, великолепно. Вы задали слишком высокую планку. Как сказал Марко, мне выпала возможность рассказать о проекте NCAP по коллизиям имен, поскольку я была сопредседателем проекта анализа коллизий имен, который изначально был предложен SSAC, но реализован дискуссионной группой со всего сообщества.

И, как сказал Марко, немногие из вас присутствовали здесь достаточно долго, чтобы помнить, но это не новый набор проблем. Мы впервые столкнулись с проблемами коллизий имен в связи с предыдущим раундом новых gTLD. Но нам пришлось вернуться к этому вопросу, потому что некоторые вещи изменились с точки зрения технологий и ожиданий в сетевой экосистеме, в которой нам приходится работать. Следующий, пожалуйста. Вернитесь на один назад.

Итак, что такое коллизия имен? Оказывается, дать определение действительно сложно, хотя ее легко узнать, когда видишь. Один из способов понять это — представить доменные имена как адреса домов. Если у двух домов один и тот же адрес, становится трудно определить, куда должна доставляться почта. Также возникают проблемы с безопасностью, если письмо доставлено не по тому адресу.

Достаточно представить последствия для конфиденциальности.

В DNS коллизии имен возникают, когда домен, используемый в глобальном пространстве имен DNS (публичный Интернет, каким мы его знаем), также используется в другом пространстве имен — например, в частной сети, управляемой вашим VPN-провайдером. В таких сетях могут использоваться разные имена, и это нормально, но когда одно и то же имя означает разные вещи, то, что вы ищете, может быть неверно истолковано. Очень быстро все становится запутанным. Следующий, пожалуйста.

Следующие несколько слайдов мы пройдем довольно быстро, чтобы избежать излишней детализации и остановимся на общих моментах. Но презентация будет доступна, и мы всегда рады обсудить технические детали.

Что не является коллизией имен? Некоторые из этих терминов будут вам знакомы, если вы внимательно изучали Руководство кандидата или материалы, связанные с новыми gTLD. Коллизии имен, например, не то же самое, что схожесть строк или сходные до степени смешения строки.

Коллизии имен — это техническая проблема, вызывающая угрозы безопасности и стабильности из-за делегирования того же самого TLD, который уже используется в частном контексте. Пример: .corp в вашей частной сети, если он совпадет с именем в публичном Интернете и будет означать

нечто иное, это чревато проблемами. Риск заключается в том, что запросы к частным именам будут утекать в публичный DNS, что также вызывает технические конфликты и сбои безопасности.

Схожесть строк — это также сложность для проекта новых gTLD, Руководства кандидата и т.д., но она скорее основана на восприятии пользователя. Это проблема пользователя, вызывающая неоднозначность из-за разных публичных TLD, которые выглядят или звучат похоже для человека. Если у вас есть .example со строчной «l» и .example с заглавной «I», человек может запутаться, что создает риск фишинга, мошенничества, потери доверия пользователей и негативных последствий для них.

Вывод: существует множество способов возникновения коллизий. Важная особенность заключается в том, что, когда компьютер сталкивается с неоднозначностью, результаты могут быть запутанными и опасными. Следующий слайд. Благодарю.

Если говорить обобщенно, то, оставляя в стороне технические детали, понимание коллизий имен важно для безопасности Интернета и напрямую связано с ответственностью ICANN за безопасность и стабильность корневой зоны DNS. Существуют риски непреднамеренных последствий, когда компании использовали имена в качестве внутренних TLD, которые могут «утекать» в глобальный Интернет.

Введение большего количества новых gTLD увеличивает вероятность возникновения таких проблем, поскольку появляется больше имен, которые уже могут использоваться в частном контексте, но при этом делегируются в публичное пространство имен Интернета.

Измерение коллизий имен является сложной задачей, и мы коснемся этого подробнее, из-за эволюции технологий и сетевой инфраструктуры с момента последнего раунда новых gTLD. Например, появились улучшения в области конфиденциальности DNS, которые затрудняют оценку происходящего. Отчасти в этом и заключается цель таких улучшений. Кроме того, альтернативные системы именования усложнили ландшафт DNS, и в целом измерения стали проводить труднее. Следующий слайд.

Я не шутила, что эти проблемы уходят корнями в прошлое. Еще один. Следующий слайд. Вот этот. Спасибо.

В 2012 году раунд новых gTLD ускорил рост корневой зоны, что вызвало вопросы о том, что произойдет при добавлении новых строк, которые уже могут использоваться в ограниченном контексте, не в публичной корневой зоне.

В 2013 году SSAC занялся этой темой и выпустил рекомендацию, указав, что в результате коллизий имен могут возникнуть значительные проблемы с безопасностью и стабильностью.

Наиболее значимые обнаруженные коллизии строк — некоторые из вас, возможно, слышали о них — это .home, .corp и .mail, которые использовались в таком множестве частных контекстов, что было собрано много данных, и выявлено множество рисков, связанных с попыткой их делегирования в глобальную корневую зону, публичную систему доменных имен.

В 2017 году Правление ICANN поручило SSAC провести комплексные исследования, чтобы все будущие делегирования gTLD могли осуществляться безопасным, стабильным и предсказуемым образом.

Проект NCAP, состоявший, полагаю, из двух отдельных исследований, стал результатом этой задачи и последующих вопросов.

В ходе финальной фазы, Исследование NCAP 2 было опубликовано в начале 2024 года, поскольку мы хотели убедиться, что полученные выводы и наши рекомендации смогут повлиять на следующий раунд новых gTLD.

Создание команды из представителей всего сообщества, а не только членов SSAC, было для нас в новинку, и, думаю, это себя оправдало. Нам удалось взять за основу предыдущие наработки и более свежие исследования и развить их. Следующий слайд.

Основной задачей проекта NCAP стал анализ текущей ситуации с выявлением и устранением коллизий имен, а также разработка рекомендаций по обновлению подходов к работе с коллизиями для предстоящего раунда новых gTLD. Результатом стала новая система оценки рисков, позволяющая не только обнаруживать коллизии имен, но и оценивать масштаб возможного ущерба, его характер, а также возможные меры по устранению или предотвращению проблем.

Следует отметить, что оценка стала сложнее по ряду причин, как мы уже упоминали. Мы уже об этом упоминали. Оказалось, что одна из главных трудностей заключается в том, что множество данных о том, какие имена ищут пользователи, которые раньше были доступны, теперь скрыто, потому что технология Janus делает для конфиденциальности пользователей гораздо больше, чем раньше. Это положительно сказывается на Интернете и пользователях, но затрудняет анализ.

Несмотря на интересные вызовы, мы смогли работать с доступными данными и достичь поставленных целей.

Цель 1: обеспечить возможность оценки коллизий имен. Мы разработали систему с поэтапным углублением анализа в зависимости от уровня риска, связанного с конкретными коллизиями.

Цель 2: предоставить ICANN процесс оценки планов по устранению и минимизации последствий выявленных коллизий имен. Мы обнаружили, что теперь, даже больше, чем раньше, каждый случай коллизии по-своему уникален. Следующий, пожалуйста.

Экзамена по этой теме не будет, но на слайде представлена схема системы из отчета NCAP Исследования 2, учитывающая риски коллизий имен и растущие сложности их выявления и устранения.

Ключевой особенностью является создание группы технического контроля для наблюдения за процессом и принятия квалифицированных решений о рисках в каждом конкретном случае. Мы исходили из того, что во многих ситуациях риски не обязательно будут постоянными.

Устранение или предотвращение проблем возможно, но поскольку все случаи уникальны, для уверенности в адекватном решении проблем коллизий потребуется значительный объем экспертной оценки. Таким образом, часть процессов в рамках этого подхода будет опираться на автоматизированные методы, а другая часть — передаваться на рассмотрение экспертной группе, аналогично практике, уже применяемой ICANN в других сложных ситуациях, где для принятия решений необходима экспертная оценка. Следующий слайд.

Таким образом, преимущества системы оценки рисков коллизий, представленной в Исследовании NCAP 2 для сообщества, включают проактивное управление рисками, которое выявляет угрозы коллизий имен и позволяет разрабатывать и оценивать стратегии их устранения до того, как они смогут нанести вред.

Мы приложили значительные усилия, чтобы сделать этот подход последовательным и эффективным. Централизованная методика анализа обеспечивает тщательную оценку рисков и их устранение для всех заявок на новые gTLD, что вновь подчеркивает ответственность ICANN за корневую зону.

Данная система, основанная на данных, позволяет принимать обоснованные решения для безопасного расширения пространства имен Интернета.

Нам также удалось решить множество проблем, связанных с конфиденциальностью в этой сфере работы. Хотя оценка коллизий имен сама по себе сопряжена с рисками, мы пришли к акцентированию того, что существует риск для конфиденциальности, связанный с неточной оценкой коллизий, когда неверные данные попадают не тем лицам или правильные данные — не тем адресатам. По нашей оценке, риск для конфиденциальности при отсутствии точного анализа коллизий имен превышает риски, связанные с проведением такой оценки.

Повторюсь, каждый случай уникален, но возможность провести сравнительный анализ рисков действий в противовес бездействию предоставляет нам дополнительный инструмент для изучения подобных ситуаций. Таким образом, мы заключаем, что раннее выявление рисков и обоснованные меры по их устранению имеют решающее значение для безопасности и стабильности DNS.

Таковы основные выводы. Если позволит время, с радостью отвечу на вопросы.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Сюзанн. Очень ценю. Мне тоже, выходит, навсегда запомнится этот урок о различии между коллизиями имен и схожестью строк. Больше не допущу этой ошибки. И я также очень рад видеть тот системный вклад [неразборчиво], который SSAC вносит в развитие этой темы на протяжении многих лет. Я вижу, что Нико поднял руку. У нас есть время на один-два вопроса. В очереди никого нет, так что, Нико, прошу.

NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]: Это краткий комментарий. Мы могли бы вернуться к слайду на странице 23? Хорошо. Итак, у нас там четыре шага, и мой вопрос касается сроков. Каково было бы среднее время? Речь идет о днях, неделях, месяцах? Я просто хотел сравнить это с 32 шагами. Помните вчерашнюю презентацию с GNSO, в

	контексте эффективности, скорости и прочего? Таким образом, в среднем, сколько времени это заняло бы?
SUZANNE WOOLF [СЮЗАНН ВУЛЬФ]:	Это как раз тот вопрос, который мы активно обсуждали, но по которому нам не удалось прийти к окончательному консенсусу в рекомендациях. Как вы правильно отметили, существуют давления в сторону максимального ускорения процесса, но мы также не хотим упустить важные риски. Поэтому мы рассматривали сроки в рамках недель, а не месяцев или лет, но этот вопрос, по сути, нам пришлось оставить на усмотрение сотрудников ICANN и сообщества для принятия окончательных решений.
MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]:	Спасибо. У нас осталось время на еще один вопрос, но я не вижу желающих в зале. В таком случае, я благодарю вас, Сюзанн, за развернутые разъяснения. Как вы сказали, слайды будут размещены онлайн.
SUZANNE WOOLF [СЮЗАНН ВУЛЬФ]:	Да.
MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]:	И мы можем перейти к следующей теме. Ее, собственно, предложили ответственные по теме злоупотреблений в DNS,

которые интересовались, смогут ли Рам и его коллеги из SSAC поделиться техническими рекомендациями или мнением относительно опубликованного документа по теме.

RAM MOHAN [РАМ МОХАН]: Спасибо, Марко. Прежде чем ответить на ваш вопрос, я хотел бы проинформировать GAC о работе, которую мы только что начали и которая связана с предыдущей темой о пространстве имен. Мы создали рабочую группу под названием «Ответственная интеграция в экосистему DNS» (RIDE). Мы сосредоточимся на том, что происходит, когда идентификаторы из других пространств имен, в частности из блокчейн-пространства, хотят связываться и взаимодействовать с идентификаторами, доменными именами и другими системами в DNS. Мы уже начали работу и планируем представить комментарии и выводы по этому вопросу.

В частности, нас интересуют и вызывают озабоченность вопросы жизненного цикла доменных имен, ввод пользователей в заблуждение, мошенничество, а также риски для безопасности и стабильности, которые могут возникнуть в самой DNS, когда системы в других пространствах имен используют термины и слова, похожие на привычное нам пространство имен, но не полностью идентичные, однако каким-то образом связанные с ним. Мы только начали работу. И будем держать вас в курсе.

Что касается вашего вопроса, Марко, на следующем слайде: мы очень рады, что начата работа над политикой по злоупотреблениям в DNS, или, по крайней мере, начата некоторая работа, и начата разработка политики в этой области. Вы можете перейти к следующему слайду.

Ранее SSAC предоставлял комментарии и рекомендации уже после формирования политических предложений. Сейчас мы меняем этот подход совместно с нашими коллегами из GNSO. Нас пригласили участвовать в этом процессе разработки политики (PDP).

Мы не участвуем в дискуссиях о том, должно ли быть одно направление работы, два, три, или они должны быть все объединены. Это вопросы для разработчиков политики. Однако мы намерены высказываться по конкретным вопросам, связанным со злоупотреблениями, делиться своими наблюдениями, особенно учитывая, что мы уделяем много времени изучению эволюции злоупотреблений и их тенденций.

Это одно из наших ключевых направлений работы. Мы считаем эту тему важной в наших диалогах с Правлением ICANN, например, при обсуждении приоритетов на 2026 год. Мы поддерживаем позицию GNSO и контрактных сторон о том, что проблема злоупотреблений в DNS должна занимать высокое место в списке приоритетов. Всегда есть конкурирующие задачи, но, если мы не справимся с этой

проблемой, пострадают не только конечные пользователи. Будет подорвана репутация саморегулируемой многосторонней модели, которую мы все считаем выдающимся примером. Мы должны действовать правильно, и борьба со злоупотреблениями в DNS должна быть одним из основных направлений работы.

Поэтому мы активно вовлечены в этот процесс и намерены участвовать в нем на этапе формирования политики гораздо более активно, чем раньше.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Рам. Это прекрасно слышать. Поскольку это открытая дискуссия, я хотел бы спросить, не хочет ли кто-то из представителей, занимающихся борьбой со злоупотреблениями в DNS, отреагировать на это? Или, возможно, есть дополнительные вопросы к SSAC по этой теме? Или, конечно, кто-либо еще, у кого есть вопросы по данной теме? Янош, Европейская Комиссия.

JANOS DRIENYOVSZKI [ЯНОШ ДРИНЬОВСКИ]: Еще раз благодарю за то, что вы здесь сегодня, и за ваши презентации. Нас немного беспокоит в процессе PDP важность определения правильного охвата. Мы вложим в это много усилий. И нас интересует ваше мнение о направлении, касающемся массовых регистраций, назовем это так, о проблеме массовых регистраций. Конечно, наша цель в итоге

процесса разработки политики — получить результат, который будет действенным и будет точно нацелен на нужные проблемы.

Мы упоминаем API, но задаемся вопросом, действительно ли такой подход полностью охватит большинство технологий или мер, позволяющих осуществлять регистрации в больших объемах. Поэтому я был бы очень благодарен за ваше мнение: является ли это хорошим подходом, или же рамки следует сформулировать так, чтобы они, конечно, обеспечивали своего рода долгосрочную актуальность подхода в конечном счете. Это мой личный интерес. Я не знаю, какие еще технологии могут существовать, которые позволяют осуществлять такие массовые регистрации. Спасибо.

RAM MOHAN [PAM MOXAH]: Спасибо. Ответ на этот вопрос требует тонкого подхода, потому что существуют примеры, когда есть законные причины для массовой регистрации. Например, компания, которая хочет защитить свой новый продукт, и регистрирует сотни доменов в разных зонах. Вопрос также в том, регистрируют ли они их во множественных TLDs, внутри одной TLD? Здесь есть свои особенности.

Хочу отметить, что доступ через API — не всегда единственный способ массовой регистрации. Мы видели множество случаев, когда люди с дурными намерениями регистрировали домены,

не используя API, как способ скрыть свою деятельность, поскольку они знают, что использование API отслеживается.

При этом я считаю, что это перспективная область для изучения. Понятие «массовые регистрации» нуждается в определении. И одно из опасений, которое мы разделяем с другими участниками сообщества, заключается в том, что если вы установите порог — скажете, что все, что ниже определенного числа, не будет проверяться с той же тщательностью, — то можно ожидать, что этой лазейкой будут злоупотреблять. Так что здесь предстоит определенная работа.

Я надеюсь, что будет разработана политика, которая обеспечит общие рамки для предотвращения нежелательного поведения, а не будет нацелена на конкретные методы, с помощью которых это поведение осуществляется. Думаю, именно этого различия нам следует стараться придерживаться в процессе разработки политики.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Рам. Я вижу, что очередь, в общем-то, пуста, что дает мне возможность перейти к следующему вопросу. И вновь я очень ценю ваши комментарии. Как вы упомянули в начале, вы будете участвовать в PDP, и мы укрепляем связи между GAC и SSAC. Это подводит нас к более общему вопросу: в чем мы видим возможности для сотрудничества? Мы, и GAC, и SSAC,

будем участвовать в этом PDP. Возможно, это не единственный путь.

Мы можем перейти к следующему слайду. Или вопрос все еще о злоупотреблениях в DNS, Индия? Или это по данному конкретному вопросу? Я вижу, что вы подняли руку.

[ИНДИЯ]: Что касается злоупотреблений в DNS в целом, я бы, пожалуй, хотел услышать мнение Рама по этому поводу. А именно: какой потенциал в снижении злоупотреблений в DNS может иметь сокращение 15-дневного срока [для установления точности]. Мы считаем, что это один из самых простых шагов, которые можно предпринять. Он может значительно помочь в снижении и смягчении последствий злоупотреблений в DNS.

Возможно, десять лет назад аутентичная проверка или верификация были бы проблемой, но сейчас эти процедуры отработаны. Мы делаем это как минимум три-четыре раза в день. Вы заселяетесь в отель — проходите аутентификацию. Вы заходите в зал ожидания аэропорта — проходите аутентификацию и верификацию. И я действительно задаюсь вопросом: как мы можем позволить кому-то получить доменное имя без даже аутентификации? И заметьте, речь идет даже не об идентификации. А лишь об аутентификации.

В связи с этим, я хотел бы услышать ваши мысли по этому поводу, поскольку я действительно чувствую, что вы

понимаете логику [неразборчиво], [почему это] вообще [предоставляется].

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо. Я понимаю, что речь идет о двухнедельном периоде между... этом двухнедельном промежутке для верификации, верно? Рам, есть ли у вас соображения по этому сроку?

RAM MOHAN [РАМ МОХАН]: Спасибо большое. Мы уже высказывались ранее по поводу срочных запросов, и, если кратко, наша позиция такова: если что-то называется «срочным», это действительно должно что-то означать. По нашему мнению, это требует очень быстрого времени реакции и не должно быть... Это эквивалент вызова экстренной службы в реальной жизни. Когда вы звоните в такую службу, вы не ожидаете ответа через 15 дней или через два рабочих дня. Таким образом, наш подход заключается в том, что это важно.

Что касается вопроса о проверке и верификации, то у SSAC, насколько я знаю, у нас нет обязательно единой, общей для всего SSAC точки зрения по этому вопросу. Однако мы отмечаем, что исследователи в области безопасности и некоторые представители правоохранительных органов заявляют, что они сталкиваются с препятствиями из-за отсутствия легкого доступа к некоторой информации о владельце домена. Поэтому мы поддерживаем разработку

систем многоуровневого доступа, которые могут предоставлять информацию сторонам, имеющим на это законные основания.

Вот, в общем, наша позиция. Мы считаем, что в отношении именно срочных запросов, особенно когда GAC и Правление работают над этим совместно, следует руководствоваться именно словарным определением слова «срочный», и «коммерчески оправданный» не должно быть базовым критерием. Спасибо.

[ИНДИЯ]: Нет, мой вопрос был не о срочных запросах. Мой вопрос касался потенциала снижения злоупотреблений в DNS за счет сокращения 15-дневного промежутка между верификацией и регистрацией домена. Я считаю, что это нечто, что в наше время действительно кажется мне непостижимым.

RAM MOHAN [РАМ МОХАН]: Да, спасибо за уточнение. Повторюсь, не могу говорить от имени всего SSAC. Но считаю, что эту область необходимо тщательно изучить. Нам следует анализировать вред для пользователей и соотносить его с другими договорными требованиями и процессами разработки политики. Однако главным приоритетом должен оставаться предотвращение вреда для пользователей.

MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]: Спасибо, Индия. Спасибо, Рам/ SSAC. Есть ли еще неотложные вопросы? У нас осталась две минуты. Я готов подвести итоги и отпустить вас на перерыв на кофе. Обратимся к слайду «Возможности будущего сотрудничества». Нико?

NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]: Спасибо, Нидерланды. У меня последний вопрос относительно сотрудничества в сфере открытого программного обеспечения. Может ли это быть частью совместной работы? Спрашиваю это потому, что на последнем IGF в Норвегии правительство Норвегии активно делилось решениями с открытым исходным кодом. И сейчас более 45 стран пользуются преимуществами этого подхода. Какой бы могла быть процедура, если бы наши уважаемые коллеги из GAC заинтересовались таким сотрудничеством? Каков был бы порядок действий?

RAM MOHAN [РАМ МОХАН]: Я бы предложил им связаться со мной как с председателем или с нашим прекрасным персоналом SSAC. Мы наладим диалог, чтобы найти оптимальные пути предоставления вам контента и другой поддержки, а также для совместной работы. Мы чрезвычайно заинтересованы в этом направлении. Это один из немногих отчетов SSAC, который создан специально для вас — так что давайте работать вместе. Мы хотим, чтобы это принесло вам пользу. И если вы действительно придете к

	сотрудничеству с нами, это станет подтверждением, что такая работа является для нас полезным начинанием.
MARCO HEGOWONING [МАРКО ХЕГОВОНИНГ]:	Спасибо. На этой ноте я хочу сердечно поблагодарить вас, Рам, Сюзанн, Маартен, Тара, за то, что снова были с нами. И, возвращаясь к теме слайда, с нетерпением жду будущего сотрудничества. Если у вас нет заключительных комментариев, Нико, думаю, мы можем идти пить кофе.
NICOLÁS CABALLERO [НИКОЛАС КАБАЛЛЕРО]:	Нет, только организационные детали. Сейчас у нас перерыв на кофе. Приятного аппетита. Мы встретимся снова в 16:30. Большое спасибо. Совещание окончено. Спасибо, Рам.

[КОНЕЦ СТЕНОГРАММЫ]