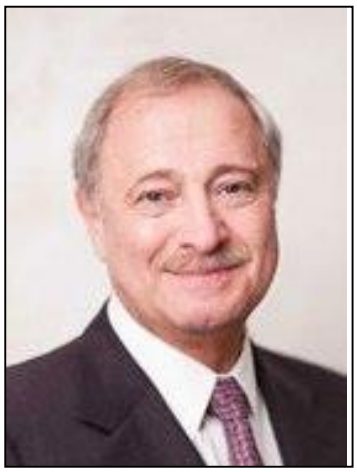
МИХАИЛ МЕДРИШ: «Совершенно бессмысленно рассматривать вопросы безопасности всего интернета вообще. Нельзя сделать закон обо всем, нужны конкретные направления, и одно из них связано с глобальной критической инфраструктурой интернета»



Михаил Абрамович Медриш
Директор, Фонд содействия развитию интернета «Фонд поддержки интернет»
Выступление на научно-практическом семинаре
«Глобальное управление интернетом: основные проблемы и задачи в 2015 году»

Для целей настоящего обсуждения я бы хотел обозначить, что Интернет – не контент. Глобальная инфраструктура интернета – это не контент. Это технологическая среда, оборудование, алгоритмы и инфраструктурные системы. Это совокупность десятков миллионов сетей. Каждая подключенная домашняя сеть – это малая сеть. И в этой сети живут миллиарды процессов, которые сами собой управляют. В этом, собственно, и есть могущество Интернета, это свойство позволяет как угодно широко масштабировать, сколько угодно сетей подключать. В какой бы момент мы не рассмотрели сеть – между двумя точками – оборудование или компьютер – подключенными к сети будет взаимодействие. Именно поэтому интернет и захватил такое большое место в нашей жизни, потому что это, с одной стороны, сложная конструкция, а с другой она очень простая.

А глобальная инфраструктура – это те технические системы, без которых эта самая конструкция жить не может. Это системы, поддерживающие уникальные номера и адреса. Также совокупность организационно-технических процедур. Понятно, что без процедур не бывает никакой технической деятельности, и процедура не есть часть технического решения как таковая. Мы говорим не только об ICANN. Пять региональных Интернет – регистратур (RIRs)

распределяют адреса и номера автономных систем. Через них появляются IP адреса у операторов связи, которые запрашивают их Local internet registries. IP адреса у них запрашивают так же и бизнес организации, которые считают, что им нужно иметь свое адресное пространство, это тоже предусмотрено процедурами. Операторы корневых серверов, которые не являются ни частями ICANN, ни частями RIR. Они независимые участники управления.

Я вижу три типа механизмов обеспечения безопасности стабильности и отказоустойчивости.:

1. Внутренние процедуры операторов систем уникальных идентификаторов.
2. Распределенность ресурсов системы. Существует 13 корневых серверов ICANN, причем каждый сервер – это не одна машина. Например, один из серверов, который стоит в университете Южной Калифорнии, – это пять машин, работающих одновременно, и еще 2 компьютера, то есть это достаточно устойчивая система. И еще почти 450 зеркал по всему миру. Система достаточно устойчивая, зеркала стоят на всех континентах кроме Антарктиды.
3. Процедура улучшения. Вся история про безопасность и стабильность по своему функциональному наполнению, по процедурам, похожа на то, что описано в ISO 9000. Нужно добиться какого-то результата, а потом постоянно улучшать, иначе начнется деградация. В ICANN есть так называемые advisory committees, которые занимаются безопасностью: Security stability advisory committee и Root server system advisory committee, куда входят представители всех владельцев корневых серверов, представитель правления ICANN. Там они рассматривают вопросы, связанные с функциональностью корневых серверов.

Наверху всего этого документ - Концепция безопасности стабильности и отказоустойчивости, которая публикуется с 2009 года и постоянно обновляется, и каждый год появляются рекомендации этих самых комитетов, которые являются источником пересмотра и выполнения каких-то действий. Начиная с 2000 года все эти системы по обеспечению безопасности работают под ICANN. ICANN держит сервер L – один сервер и 146 зеркал, то есть треть по всему миру.

Вторым активном участником являются региональные Интернет- регистратуры (RIRs), первый RIPE NCC появился в 1992 году, а последний AFRINIC в 2005. Это все некоммерческие организации, зарегистрированные на соответствующих континентах. Появление RIRs было изложено в RFC в августе 1990 года и его автор Винт Серф (Vint Cerf). В нем написано – так как интернет развивается достаточно активно, необходима интернационализация процессов распределения адресов. И на базе этого запроса мы имеем теперь 5 RIRs, которые в 2003 году для координации своей деятельности создали организацию NRO, которая подписала соответствующее соглашения о взаимопонимании с ICANN, образовала Address Support Organization внутри ICANN. Таким образом, они отвечают на вопросы, связанные с безопасным функционированием системы распределения IP адресов, а также ведут и базу данных адресов. Когда мы, заходя на какой-нибудь сервис, видим указание своего местоположения, запрашивается база данных в соответствующем RIRe, где все распределенные

адреса учтены и записаны, какому оператору они принадлежат и какому потребителю выданы, стоит место расположение этого оператора, и достаточно точно определяет геолокацию человека. Роль RIRs не только в том, чтобы выдать адрес, они еще держат базу данных и открытый доступ к ней обеспечивают, для того чтобы весь мир мог ей пользоваться, и отчетливо понимать в деталях, все что там доступно.

Какие я вижу риски для безопасности стабильности? В целом, есть технические риски – я уже показал, как их можно преодолевать в глобальной инфраструктуре. Человеческий фактор всегда есть, он минимизируется путем многократного дублирования с одной стороны, с другой стороны – это процедура смены шифровальных ключей в DNS системы в Verisign, где присутствуют security officers от RIRs. Третья группа рисков – это политические. На мой взгляд, сегодня политические риски самые существенные, они сильно превышают все остальное вместе взятое. И возможное следствие политических рисков - это фрагментация глобальной сети и введение отдельных DNS и ведения отдельного закрытого адресного пространства. Как следствие - это фрагментация и затруднение для отдельных стран коммуникаций в интернете, не только для тех, кто вводит ограничения, но и для тех, кто стоит «за» ними. Ну и в конечном итоге снижение роли Интернета как катализатора инновационного развития. Безусловно, важен вопрос безопасности. С помощью Интернета совершаются преступления, и это очевидно, но надо уметь жить с Интернетом.

Мои предложения по снижению уровня этих рисков:

1. Инициировать рассмотрение на уровне ООН вопроса конвенции о технической глобальной инфраструктуре Интернета – чего нельзя делать. Это должно быть зафиксировано в виде soft law – то, что не является нормативными международными актами, а имеется де-факто. На мой взгляд, совершенно бессмысленно и контрпродуктивно рассматривать вопросы безопасности всего Интернета вообще. Это ни о чем. На этом пути никакого решения найти не возможно. Нужно использовать системный анализ, потому что нельзя сделать закон обо всем, нужны конкретные направления. Одно из них связано с глобальной критической инфраструктурой интернета. К тому же это созвучно текущему процессу передачи полномочий NTIA. Но здесь нельзя решать этот вопрос без такого главного актора, как правительство США и ICANN как исполнителя контракта. Но это должно быть международное соглашение, страны должны согласиться. Особенно те, для которых слово суверенитет является критически важным.

2. Необходимы переговоры между ISOC и IETF, с одной стороны, и МСЭ, с другой. История отношений IETF и МСЭ насчитывает больше 20 лет, и это нельзя не учитывать. Нельзя взять, и передать все технические вопросы в МСЭ. Это загонит ситуацию в тупик. 20 лет назад велись переговоры, чтобы под зонтик МСЭ передать всю нормативную деятельность, связанную с развитием Интернета. И тогда представители МСЭ встали на не очень правильные позиции силы, аргументируя тем, что их стандарты электросвязи уже закреплены в ISO, а технические стандарты передачи данных в сети Интернет не закреплены. Теперь обе

стороны ушли дальше друг от друга, и договориться будет сложнее. Вместо того, чтобы настаивать, у кого должны быть функции, надо попытаться объединить усилия, ментальные процессы. Ведь в конечном итоге, все делают люди. А новую площадку я вижу в виде ФУИ с новым мандатом. Конечно, ФУИ не может быть источником международного права, но готовить документы он вполне может. Спасибо!