Концепция безопасности, стабильности и отказоустойчивости

ICANN — всемирная организация, которая координирует работу систем уникальных идентификаторов Интернета, действуя на благо пользователей во всем мире, обеспечивая функционирование единого оперативно совместимого Интернета.

Март 2013 г.

Содержание

Список иллюстраций

Сводное резюме

Интернет представляет собой процветающую экосистему, которая объединяет множество заинтересованных сторон на основе сотрудничества в открытой и прозрачной среде. Интернет способствует обмену знаниями, творчеству и торговле в рамках общей глобальной среды. Возможность взаимодействия в рамках этой среды зависит от функционирования и координации систем уникальных идентификаторов Интернета, от его стабильности и отказоустойчивости, а также от здоровья его экосистемы.[1]

ICANN и операторы этих систем осознают, что сохранение и повышение безопасности, стабильности и отказоустойчивости этих систем является ключевым элементом их сотруднических отношений.

С 2009 года ICANN публикует ежегодную Концепцию безопасности, стабильности и отказоустойчивости (БСО). Концепция признана в «Подтверждении обязательств»[2] и получила положительную оценку Группы проверки безопасности, стабильности и отказоустойчивости[3] в процессе проверки, предусмотренной «Подтверждением обязательств».

Концепция БСО описывает роль и рамки компетенции ICANN как организации, поддерживающей единый, всемирный, оперативно совместимый Интернет, а также проблемы, стоящие перед системами уникальных идентификаторов Интернета. Этот документ состоит из двух частей. В части А излагается обоснование роли ICANN в обеспечении безопасности, стабильности и отказоустойчивости, даются определения экосистемы Интернета и сообщества ICANN. В части Б излагаются стратегические задачи с точки зрения обеспечения БСО и мероприятия, запланированные на 2014 ФГ (июль 2013 г. — июнь 2014 г.).

Основные отличия Концепции на 2014 ФГ от Концепции на 2013 ФГ отражают утверждение рекомендаций ГП БСО в октябре 2012 года[4] и реакцию на изменения в экосистеме Интернета с момента публикации предыдущей версии в июне 2012 г. (см. часть Б). Мероприятия, планируемые в 2014 ФГ, будут сосредоточены на поддержании здоровья экосистемы с целью создания фундамента для более стабильного, надежного и отказоустойчивого Интернета во благо мирового сообщества.

---

[1] Согласно своему Уставу, корпорация ICANN координирует распределение и назначение трех наборов уникальных идентификаторов Интернета: доменные имена (формирующие систему DNS); адреса интернет-протокола (IP) и номера автономных систем (AC); а также номера портов протокола и параметров.

[2] «Подтверждение обязательств» — документ, подписанный Министерством торговли США и ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[3] Итоговый отчет Группы проверки безопасности, стабильности и отказоустойчивости от 20 июня 2012 г., http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

[4] Утверждение рекомендаций группы проверки БСО Правлением ICANN 18 октября 2012 года, http://www.icann.org/en/about/aoc-review/ssr/board-action.

Концепция на 2014 ФГ будет представлена в качестве единого документа для облегчения ее перевода и распространения на предстоящей конференции ICANN в Пекине 7-11 апреля 2013 г.

Часть А — Обоснование роли ICANN

Миссия и основные ценности ICANN

> «Миссией ICANN является координирование на высшем уровне глобальных систем уникальных идентификаторов Интернета и, в частности, обеспечение стабильного и безопасного функционирования уникальных идентификаторов Интернета».
>
> Устав ICANN с поправками от 20 декабря 2012 года (http://www.icann.org/en/about/governance/bylaws#I)
>
> Основная ценность № 1 — Сохранение и повышение эксплуатационной стабильности, надежности, безопасности и глобальной оперативной совместимости Интернета.

Эта основная ценность отражена в «Подтверждении обязательств», а именно: «для обеспечения оперативной совместимости требуется глобальная техническая координация фундаментальной инфраструктуры Интернета — DNS» и далее: «сохранение безопасности, стабильности и отказоустойчивости DNS» является одним из важнейших обязательств выполняемых во благо пользователей Интернета по всему миру.

Роль и сфера компетенции CANN в обеспечении БСО

По результатам проверки, предусмотренной «Подтверждением обязательств», группа проверки безопасности, стабильности и отказоустойчивости рекомендовала ICANN «опубликовать единое, четкое и непротиворечивое заявление о своей сфере компетенции в обеспечении БСО и выполнении ограниченной технической миссии». (Рекомендация 1 от 20 июня 2012 г.).

Проект заявления о роли и компетенции ICANN в обеспечении безопасности, стабильности и отказоустойчивости уникальных идентификаторов Интернета был опубликован в мае 2012 года (http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm) и пересмотрен после общественного обсуждения и сбора отзывов на конференциях ICANN в Праге (июнь 2012 г.) и Торонто (октябрь 2012 г., http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf).

Нижеследующее описание роли и сферы компетенции ICANN приведено в рамках выполнения Рекомендации 1:

> В качестве всемирной организации с многосторонним участием ICANN способствует безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета за счет координации и сотрудничества.

Сообщество ожидает от ICANN, как от всемирной организации, выполнения ею своей роли в соответствии с принципами открытости, подотчетности и прозрачности с учетом разнообразия заинтересованных сторон в рамках более широкой экосистемы Интернета.

В рамках технической миссии ICANN ее роль в обеспечении БСО включает три категории обязанностей:

1. Эксплуатационные обязанности ICANN (управление организационными рисками внутренней деятельности, включая функционирование корневого сервера «L» и DNS, операции подписания ключей DNSSEC, функции IANA, деятельность в отношении новых ДВУ, управление базой данных часовых поясов);
2. Участие ICANN как координатора, партнера и организатора в международном сообществе при решении политических и технических вопросов, относящихся к уникальным идентификаторам Интернета;
3. Сотрудничество ICANN с другими участниками глобальной экосистемы Интернета.

Рис. 1 — Техническая миссия ICANN

Определение терминов, используемых в данной Концепции

Безопасность — способность защищать уникальные идентификаторы Интернета и предотвращать их неправомерное использование.

Стабильность — способность обеспечивать ожидаемое функционирование системы и доверие к ней у пользователей уникальных идентификаторов.

Отказоустойчивость — способность системы уникальных идентификаторов эффективно выдерживать/переносить злонамеренные нападения и прочие деструктивные события без нарушения или приостановки обслуживания.

Примечание — Эти определения остались без изменений со времени опубликования в 2011 году Концепции БСО на 2012 ФГ.

На основании результатов работы 2-го симпозиума по безопасности DNS (состоявшегося в Киото, Япония, в 2010 году) и 3-го симпозиума по безопасности DNS (состоявшегося в Риме, Италия, в 2011 году) в Концепцию БСО на 2014 ФГ было включено первоначальное определение термина **здоровье уникальных идентификаторов**. Это понятие является измененным вариантом определения, приведенного в докладе Киотского симпозиума, и звучит следующим образом:

> Общее состояние функционирования уникальных идентификаторов Интернета, находящееся в номинальных технических пределах с точки зрения согласованности, целостности, скорости, доступности, уязвимости и отказоустойчивости.

В экологической экономике понятие «здоровье экосистемы» определяется как «показатель работы сложной системы в целом, определяемый поведением ее составляющих».[5]

К обязанностям, выходящим за рамки роли ICANN в обеспечении БСО, относятся следующие:

- ICANN не выполняет роль органа обеспечения правопорядка в Интернете или оперативного противодействия криминальной деятельности;
- ICANN не участвует в использовании Интернета для киберразведки и кибервойны;
- ICANN не участвует в определении составляющих противозаконного поведения в Интернете.

ICANN как организация не является правоохранительным органом, судом общей юрисдикции или правительственным агентством. Правоохранительные органы и правительства участвуют в работе ICANN и разработке политики в качестве заинтересованных сторон.

[5] Данное определение создано на основе материалов статьи Роберта Костанца и Майкла Маго «Что такое здоровая экосистема?» (Robert Costanza, Michael Mageau «What is a healthy ecosystem?») из института экологической экономики Университета штата Мэриленд, напечатанной в 1999 г. в журнале Aquatic Ecology, http://geminis.dma.ulpgc.es/profesores/personal/jmpc/Master08%28PrimeraEdici%F3n%29/Homeostasis/Homeo03s.pdf, http://books.google.com/books?id=YTeCxF5gqMQC&dq=ecosystem+and+health. На формулировку данного определения также оказала влияние опубликованная в 2004 году статья «Концепция анализа устойчивости социально-экологических систем с точки зрения институциональной теории» («A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective»), http://www.ecologyandsociety.org/vol9/iss1/art18/.

ICANN действительно играет некоторую роль в поддержке законных действий правоохранительных органов или правительственных агентств по их требованию. ICANN вместе с сообществом специалистов по операционной безопасности принимает участие в изучении, анализе и выявлении фактов злонамеренного использования или злоупотребления DNS.

ICANN не может в одностороннем порядке приостанавливать или аннулировать регистрацию доменных имен. ICANN способна обеспечивать соблюдение своих договоров с третьими лицами, включая поставщиков услуг регистрации доменных имен.

В отношении протоколов Интернета ICANN играет такую же роль, что и любая другая заинтересованная сторона; развитие протоколов Интернета и соответствующих стандартов не входит в сферу компетенции ICANN. ICANN поддерживает разработку открытых стандартов посредством коллективной работы с многосторонним участием.

Актуальные проблемы

Неправомерное использование и атаки на DNS и глобальные сети ставят под угрозу общую безопасность систем уникальной идентификации. Целью атак на DNS является широкий круг пользователей, физические лица, коммерческие организации, гражданское общество и правительства.

В свете увеличения частоты и изощренности фактов агрессии и других видов злонамеренного поведения корпорация ICANN и мировое сообщество должны продолжать совместную работу, направленную на обеспечение здоровья экосистемы, повышение отказоустойчивости систем уникальной идентификации и укрепление их возможностей.

Деятельность в Интернете отражает полный спектр человеческих мотиваций и моделей поведения. Частично такая деятельность отражает открытый характер Интернета, принесший ему успех, позволивший внедрить передовые нововведения и способствовавший обмену знаниями, творчеству и торговле в общей глобальной среде.

В современной среде совместного многостороннего управления Интернетом в более широких рамках экосистемы Интернета традиционный взгляд, подразумевающий, что работу по кибербезопасности возглавляет какой-то один сектор, будь то правительства или частный сектор, уже не актуален. Ни правительства, ни отдельные субъекты в частном секторе не обладают соответствующими административными или правовыми полномочиями для управления различными группами взаимосвязанных систем и сетей, а масштаб задачи управления этими ресурсами и обеспечения их безопасности позволяет решить ее лишь совместными усилиями множества сторон.

Все стороны, заинтересованные в обеспечении кибербезопасности, должны шире смотреть на эту проблему. Вопросы обеспечения безопасности с точки зрения уникальных идентификаторов Интернета следует решать посредством обеспечения здоровья экосистемы Интернета. В центре такого подхода — жизнеспособный или здоровый, стабильный и отказоустойчивый Интернет. То есть система, которая будет жизнеспособной и в будущем. Нам нужно вместе сосредоточиться на обеспечении

«способности экосистемы сохранять свою структуру и работоспособность на протяжении времени при воздействии на нее внешних факторов».[6]

За прошедший год выросло количество угроз для систем уникальных идентификаторов Интернета. В 2012 году в новостных СМИ появлялись сообщения об атаках на операторов реестров доменов верхнего уровня (см. заявление IEDR за ноябрь 2012 г. https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf и опубликованную в ноябре 2012 г. в *Techcrunch* статью о PKNIC, http://ta.gg/5uf), регистраторов, банковский сектор, правоохранительные органы и об угрозах для операторов корневых серверов. См. доклад Arbor Networks по безопасности всемирной инфраструктуры, январь 2013 г., http://www.arbornetworks.com/research/infrastructure-security-report.

В результате вмешательства правительства пользователи лишались связи с внешним миром, например, в Сирии (см. http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml). Ураган «Сэнди» нанес ущерб каналам доступа в Интернет на северо-востоке Соединенных Штатов, показав тем самым уязвимость глобальных сетей перед природной стихией (см. Предварительный анализ отказов сети во время урагана «Сэнди», технический отчет USC/ISI ISI-TR-685b, ноябрь 2012 г., ftp://ftp.isi.edu/isi-pubs/tr-685.pdf).

Проявились и некоторые тенденции, тормозящие процесс оздоровления уникальных идентификаторов, включая медленные темпы внедрения DNSSEC регистраторами, разработчиками браузеров и приложений, а также владельцами регистраций. Повышение осведомленности об использовании DNS в преступных целях стимулировало интерес к разработке тактики и инструментов, позволяющих бороться с этими угрозами.

Кроме того, наблюдаются и другие тенденции:

- Продолжается увеличение числа операторов ДВУ, внедряющих DNSSEC.
- Растет количество экземпляров корневых серверов в мировом масштабе.
- Введены в эксплуатацию дополнительные новые нДВУ (с ИДИ и без ИДИ), охватывающие все большее количество языков и наборов символов.
- Наблюдается дальнейший прогресс в оценке заявок, поступивших в рамках программы внедрения новых рДВУ, и в 2013 году ожидается ввод новых рДВУ в эксплуатацию.
- Растет интерес к наращиванию возможностей обеспечения кибербезопасности, стимулирующий изучение DNS не только эксплуатационными сообществами, но также правоохранительными органами и юристами.

[6] Констанца, Маго и др.

Экосистема Интернета и Сообщество ICANN

ICANN работает на благо интернет-сообщества в целом. Общество — это совокупность разнообразных сообществ, связанных Интернетом и работающих как одна сложная экосистема. В настоящий момент Интернет стал одним из основных факторов, обеспечивающих обмен знаниями и информацией, коммерческие операции и функции управления в мировом масштабе. Заявление ЮНЕСКО в Ванкувере, декабрь 2012 г., (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) и ВВИО+10, «К обществам, основанным на знаниях, во имя мира и развития» («Toward Knowledge Societies for Peace and Development»), итоговое заявление, 27 февраля 2013 г. (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

Интернет признается в качестве основополагающего фактора, обеспечивающего поддержку мировой экономики и сохранение устойчивого развития (см. документ ОЭСР «Перспективы интернет-экономики в 2012 году» («Internet Economy Outlook 2012») http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

Термин «экосистема» описывает окружающий нас мир природы. Он может быть определен как сеть взаимодействия организмов между собой и с окружающей их средой. Экосистемы являются динамическими объектами. Интернет — экосистема и одновременно сеть организаций и сообществ. Эти организации и сообщества участвуют в совместной работе, выполняя свои функции. Причиной успеха и бурного развития Интернета являются такие свойства его экосистемы, как открытость, прозрачность и готовность к сотрудничеству.

Экосистема Интернета состоит из ряда организаций и процессов, формирующих схему координации и управления всемирного Интернета и обеспечивающих его комплексное функционирование. Этими организациями являются: технические и инженерные организации, операторы сетей, организации управления ресурсами, пользователи, гражданское общество, коммерческие и некоммерческие организации, образовательные учреждения, директивные органы, правоохранительные органы и правительства.

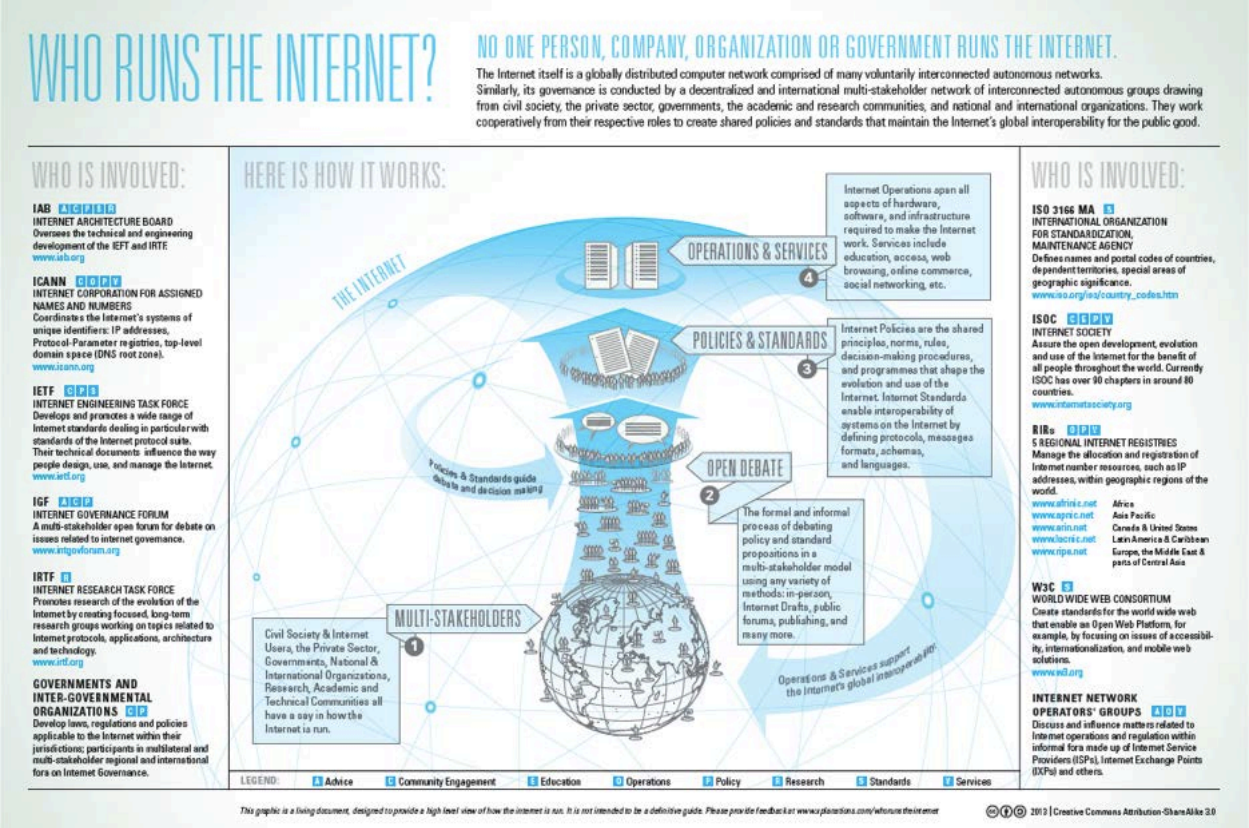


Рис. 2 — Графическое представление экосистемы Интернета

С точки зрения ICANN, экосистему Интернета можно представить в виде трехуровневой структуры:

- мировое сообщество,
- сообщество ICANN,
- и ICANN как одна из организаций.

В мировое сообщество входят те, кто полагается на здоровую, стабильную и надежную систему уникальных идентификаторов как на инструмент для обмена знаниями, торговли и инноваций, но, возможно, не знает об ICANN или не участвует в ее деятельности.

Сообщество ICANN охватывает более широкое сообщество субъектов, участвующих в программах, процессах и мероприятиях ICANN, которые приводят в действие модель разработки политики с многосторонним участием во благо пользователей всемирного Интернета.

ICANN как организация — это оперативные структуры, функции и вспомогательный персонал, которые помогают более широкому сообществу ICANN и заинтересованным сторонам координировать уникальные идентификаторы Интернета.

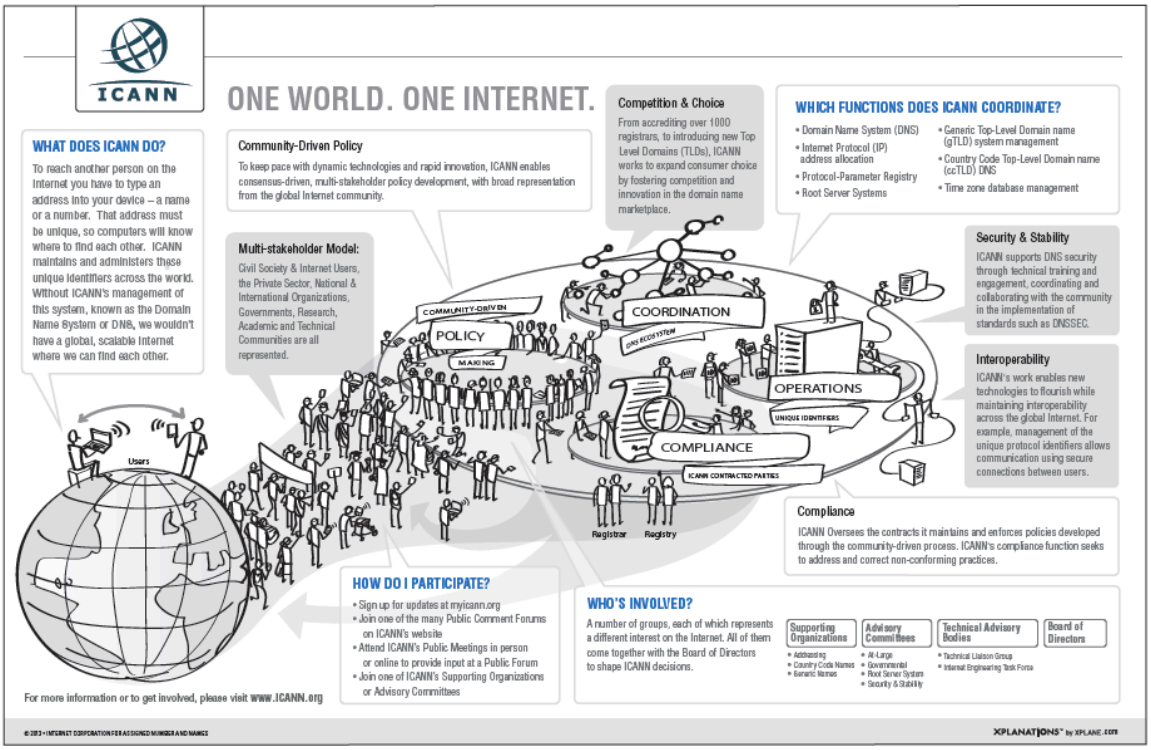


Рис. 3 — Графическое представление ICANN

Полноформатную версию приведенной выше схемы размером 11x17 дюймов (279,4x431,8 мм) можно получить на 6 языках на сайте https://community.icann.org/display/ISBM/Handouts+for+Speakers+Bureau. Сообщество участвует в работе ICANN через группы заинтересованных сторон и постоянные группы, организации поддержки и консультативные комитеты. Информацию о консультативных комитетах можно найти на их страницах по приведенным ниже ссылкам:

1. Расширенный консультативный комитет — http://www.atlarge.icann.org/alac
2. Правительственный консультативный комитет — https://gacweb.icann.org/
3. Консультативный комитет системы корневых серверов — http://www.icann.org/en/groups/rssac
4. Консультативный комитет по безопасности и стабильности — http://www.icann.org/en/groups/ssac

Эти комитеты консультируют Правление ICANN, вносят свой вклад в процессы разработки политики и поддерживают вовлечение сообществ в работу.

В процессе разработки политики участвуют три организации поддержки:

1. Организация поддержки адресов (ОПА) — http://aso.icann.org/ (IP-адреса)
2. Организация поддержки национальных имен (ОПНИ) — http://ccnso.icann.org/ (нДВУ)
3. Организация поддержки родовых имен — http://gnso.icann.org (рДВУ)

За 15 лет, прошедших с момента создания ICANN в 1998 году, размер DNS вырос с нескольких сотен тысяч доменных имен, распределенных между семью родовыми доменами верхнего уровня и примерно 25000 национальных ДВУ, до более чем 250 миллионов доменных имен, используемых 2,5 миллиардами пользователей Интернета в 316 ДВУ. Это пространство должно резко увеличиться с вводом новых родовых ДВУ в 2013 году.

На март 2013 года в корневой зоне находится 316 делегированных ДВУ. На представленной ниже схеме показано, на какие категории делятся эти ДВУ.

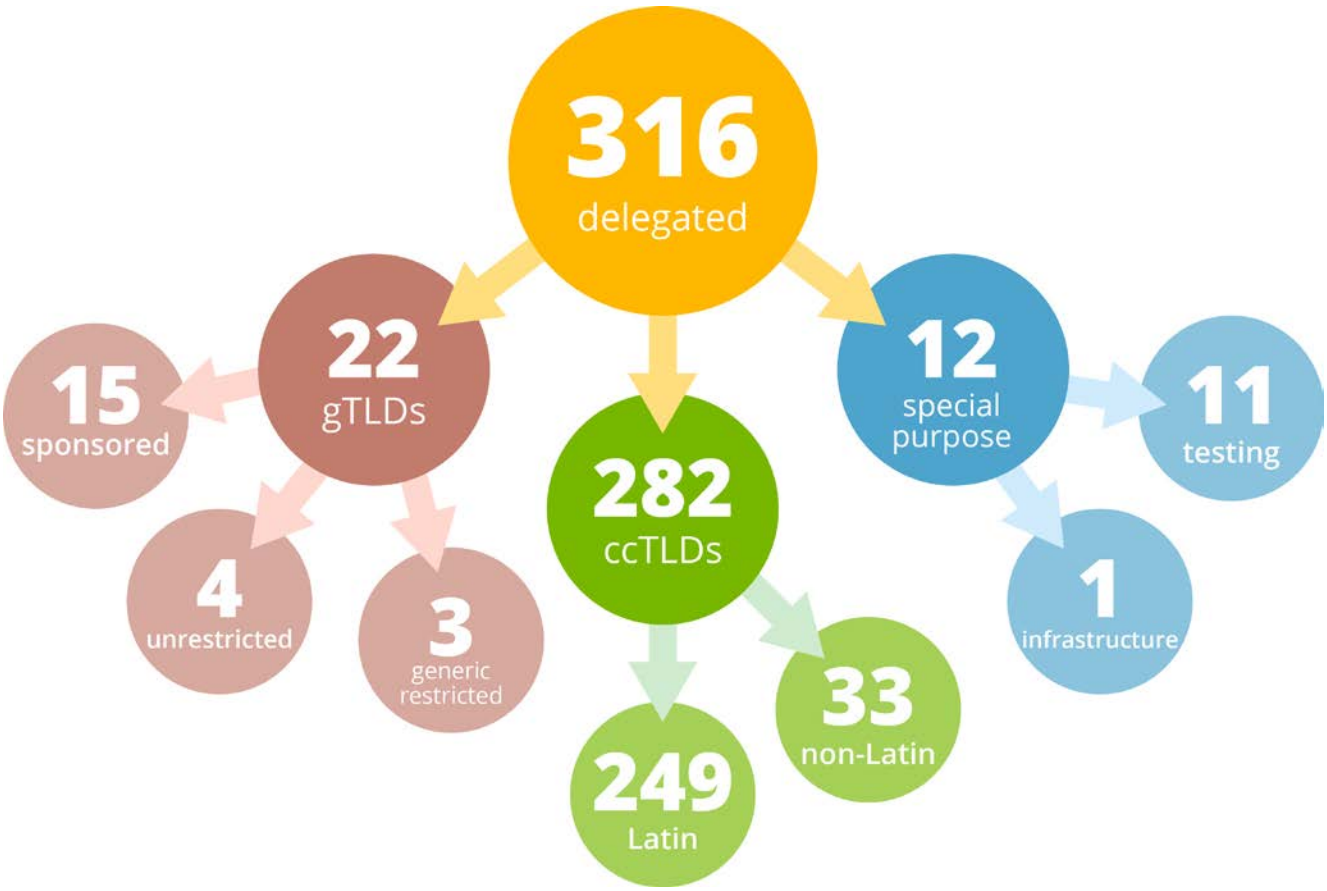


Рис. 4 — ДВУ в корневой зоне (схема предоставлена Кимом Дэвисом (Kim Davies), IANA)

Взаимоотношения в сфере БСО

ICANN поддерживает взаимоотношения со сторонами, связанными с ICANN договорными обязательствами (реестрами и регистраторами доменных имен, поставщиками услуг депонирования и другими лицами), находящимися с корпорацией в партнерских отношениях, подписавшими меморандумы о взаимопонимании, рамочные соглашения о подотчетности или соглашения, заключаемые путем обмена письмами. Прочие связи между ICANN и другими международными организациями или заинтересованными сторонами в экосистеме могут носить менее официальный или несистемный характер. https://www.icann.org/en/about/agreements.

Стороны, участвующие в процессе регистрации доменных имен должны действовать сообща, чтобы принимаемые решения, связанные с глобальной технической координацией уникальных идентификаторов Интернета, работали на благо общества и были подотчетными и прозрачными.

Приведенная ниже схема отображает природу взаимоотношений в процессе регистрации доменов.

В соответствии с Рекомендациями 4 и 5 группы проверки БСО ICANN в настоящий момент находится в процессе документирования и выработки определения характера своих взаимоотношений с сообществом ICANN с точки зрения обеспечения БСО. Это поможет найти единую платформу для понимания взаимосвязей между различными организациями и субъектами в рамках выполняемых ими функций и позволит ICANN поддерживать эффективные рабочие процедуры, способствующие достижению целей ICANN в отношении БСО и решению соответствующих стратегических задач.

Часть Б — Модуль БСО на 2014 ФГ

В этом разделе Концепции безопасности стабильности и отказоустойчивости говорится о планируемых мероприятиях и инициативах в области БСО на 2014 финансовый год, охватывающий период с 1 июля 2013 года по 30 июня 2014 года.

Вопросы безопасности в стратегическом плане ICANN

В стратегическом плане ICANN стабильность и безопасность DNS указаны в качестве одной из четырех важнейших стратегических сфер деятельности организации. Это соответствует той важной роли, которая уделяется БСО в «Подтверждении обязательств». Широкий диапазон обязанностей ICANN по обеспечению безопасности, стабильности и отказоустойчивости разделен на стратегические задачи, работу сообщества, стратегические проекты и работу персонала.

Стратегический план ICANN на 2012-2015 гг. для 2013 года останется без изменений (см. https://www.icann.org/en/news/announcements/announcement-28jan13-en.htm). Это тот же стратегический план, который был опубликован до обнародования Концепции БСО на 2013 ФГ (в июне 2012 года). Предложения и комментарии, полученные в рамках цикла планирования на 2013 год, показали, что у сообщества по-прежнему существует потребность в обучающих программах и мероприятиях по наращиванию потенциала. Это говорит о поддержке технического сотрудничества со стороны отдела безопасности ICANN.

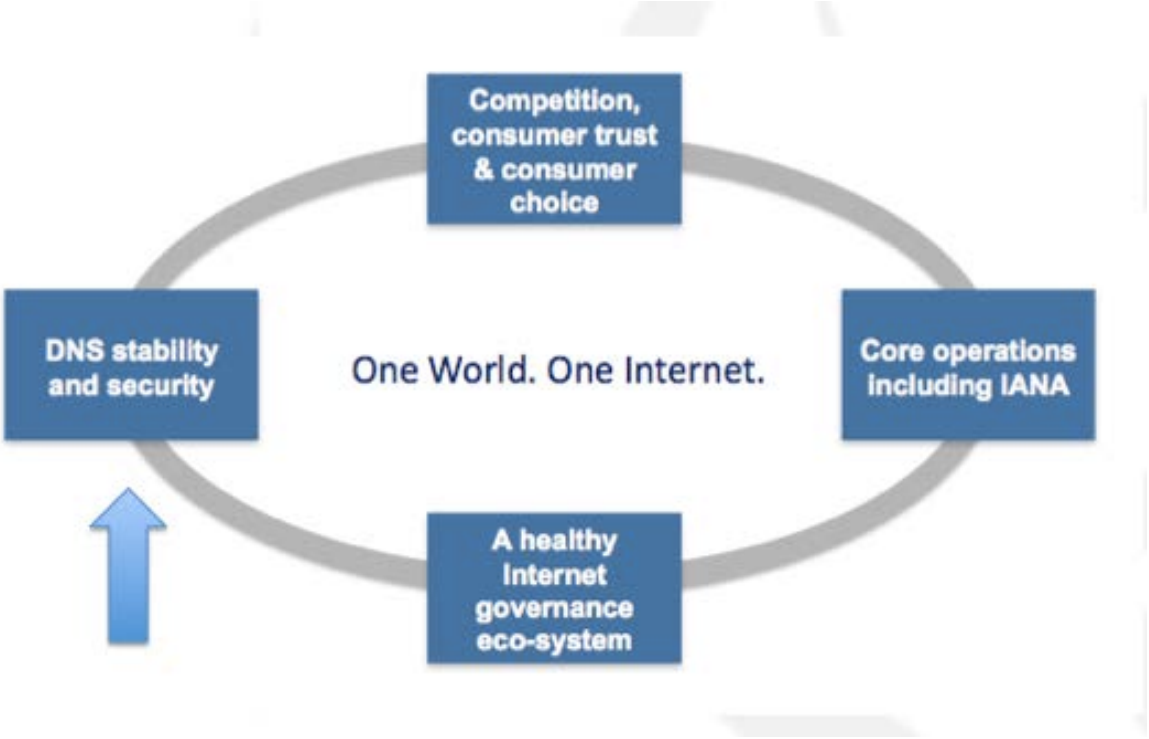


Рис. 5 — Стратегический план ICANN

В стратегическом плане на 2012-2015 гг. изложены следующие 5 стратегических задач в отношении обеспечения безопасности и стабильности DNS:

1. Сохранение и обеспечение работоспособности DNS
2. Улучшение управления рисками и отказоустойчивости DNS, IP-адресов и параметров
3. Содействие широкому признанию DNSSEC
4. Расширение международного сотрудничества в области DNS
5. Улучшение мер реагирования на происшествия в сфере безопасности DNS

ICANN начнет процесс стратегического планирования, сосредоточив свои усилия на разработке долгосрочного плана на следующие пять лет, начиная с июня 2013 года. Более подробно об этом новом подходе будет сообщено дополнительно. Поскольку вопросы безопасности являются для ICANN основополагающими, безопасность, стабильность и отказоустойчивость уникальных идентификаторов будут оставаться одним из ключевых стратегических направлений для этой организации.

Проверка, предусмотренная документом «Подтверждение обязательств»

В «Подтверждении обязательств», подписанном корпорацией ICANN и Министерством торговли США 30 сентября 2009 г. (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm), сохранение безопасности, стабильности и отказоустойчивости DNS признается в качестве ключевого обязательства (Раздел 3b).

«Подтверждение обязательств» также «регламентировало и документально зафиксировало осуществление технической координации системы доменных имен и адресов Интернета (DNS) на мировом уровне организацией, представляющей частный сектор».

В разделе 9.2 документа «Подтверждение обязательств» констатируется, что ICANN утвердила план обеспечения безопасности, стабильности и отказоустойчивости (БСО), который будет регулярно обновляться в свете новых угроз, возникающих для DNS (включая уникальные идентификаторы). Данный план будет пересматриваться не реже чем раз в три года.

Первая проверка БСО, проведенная в июне 2012 года, «выявила области, в которых ICANN демонстрирует успешную работу, области, в которых возможны улучшения, а также другие области, в которых следует определить и внедрить ключевые элементы БСО». Итоговый отчет ГП БСО, июнь 2012 г.

Правление ICANN одобрило итоговый отчет и рекомендации в октябре 2012 года.[7] Со времени проведения конференции ICANN в Торонто ICANN продвинулась вперед с точки зрения выполнения рекомендаций группы проверки БСО.

Обновленная информация о ходе выполнения рекомендаций корпорацией ICANN опубликована 19 декабря 2012 г. (http://blog.icann.org/2012/12/tracking-the-ssr-review-implementation/). Две рекомендации уже выполнены (Рекомендации 18 и 24). В течение оставшейся части 2013 ФГ, до 2015 ФГ включительно и до начала следующей процедуры проверки БСО ICANN будет следить за реализацией ее результатов наряду с результатами других проверок по «Подтверждению обязательств». (http://www.icann.org/en/news/in-focus/accountability).

Двадцать восемь рекомендаций были согласованы со структурой управления ICANN, представленной на конференции ICANN в Торонто. Это:

- Констатация цели [рекомендации 1, 2, 18, 24]
- Совершенствование деятельности [рекомендации 7, 8, 17, 20, 21, 9, 10, 11, 22, 25, 26, 27, 15, 28]
- Интернационализация [рекомендации 3, 4, 5, 14, 16]
- Развитие модели многостороннего сотрудничества [рекомендации 6, 12, 13, 19, 23]

Более подробную информацию о выполнении отдельных рекомендаций можно найти в приложении А. «Предыдущие планы и концепции ICANN по БСО» на 2010, 2011, 2012 и 2013 финансовые годы доступны по адресу https://www.icann.org/en/about/staff/security/archive.

[7] http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e

Новый сезон — на пути к матричной организационной структуре

В октябре 2012 года на конференции ICANN в Торонто генеральный директор ICANN Фади Шехаде (Fadi Chehade) представил новую структуру управления ICANN. Она предполагает ведение деятельности ICANN с использованием матричной организационной структуры. Отдел безопасности является одной из технических служб ICANN наряду с входящими в состав корпорации отделами IANA, ИТ и оперативным отделом DNS.

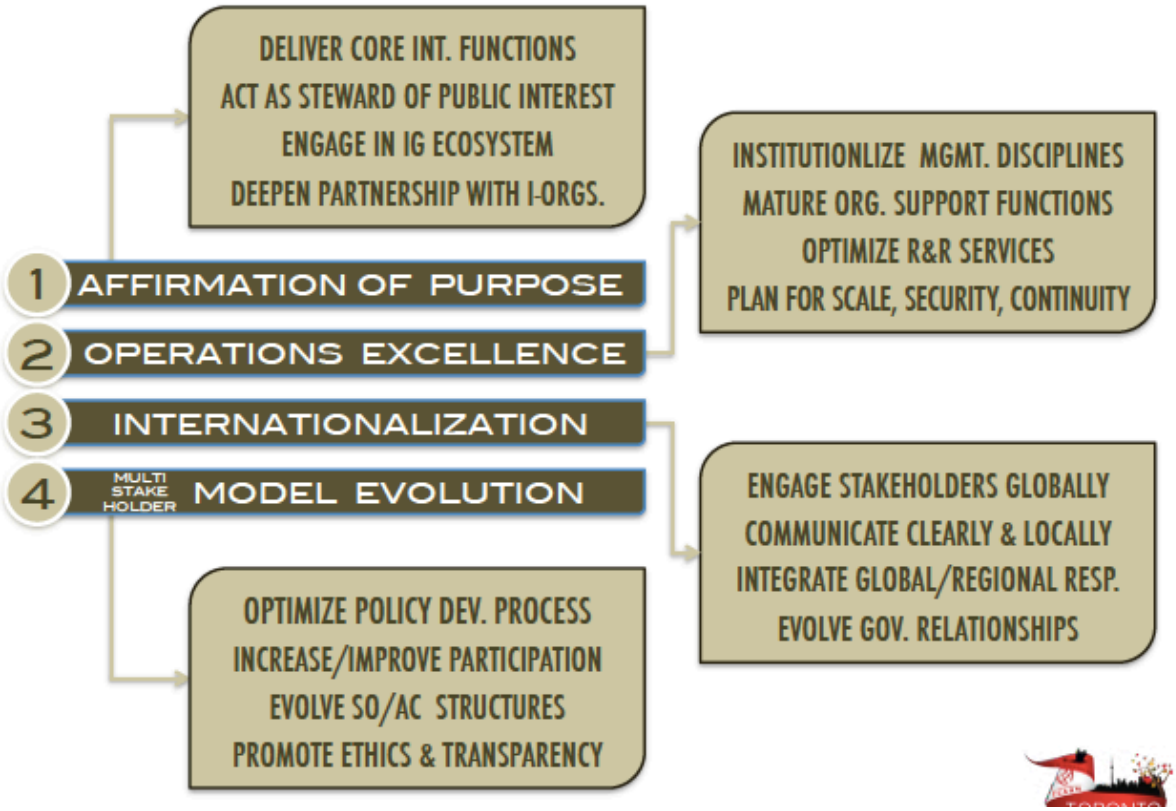


Рис. 6 — Сферы управления ICANN

Деятельность отдела безопасности охватывает всю организацию, поддерживая каждую из 4 сфер управления. Это включает поддержку программы совершенствования деятельности, работы отдела международного взаимодействия с заинтересованными сторонами ICANN (GSE) с точки зрения интернационализации и развития модели многостороннего участия, а также стимулирования более широкого обсуждения вопросов управления Интернетом в рамках более широкого сообщества.

Матричная модель будет внедряться путем распределения деятельности ICANN между тремя основными центрами — в Лос-Анджелесе, Сингапуре и Стамбуле. ICANN будет также поддерживать работу отделений по вовлечению заинтересованных сторон в Брюсселе, Вашингтоне и других местах, что позволит корпорации стать ближе к заинтересованным сторонам.

Графическое представление деятельности отдела безопасности ICANN

Приведенная ниже схема позволяет лучше представить деятельность ICANN по обеспечению безопасности, стабильности и отказоустойчивости как составляющую роли и сферы компетенции корпорации.

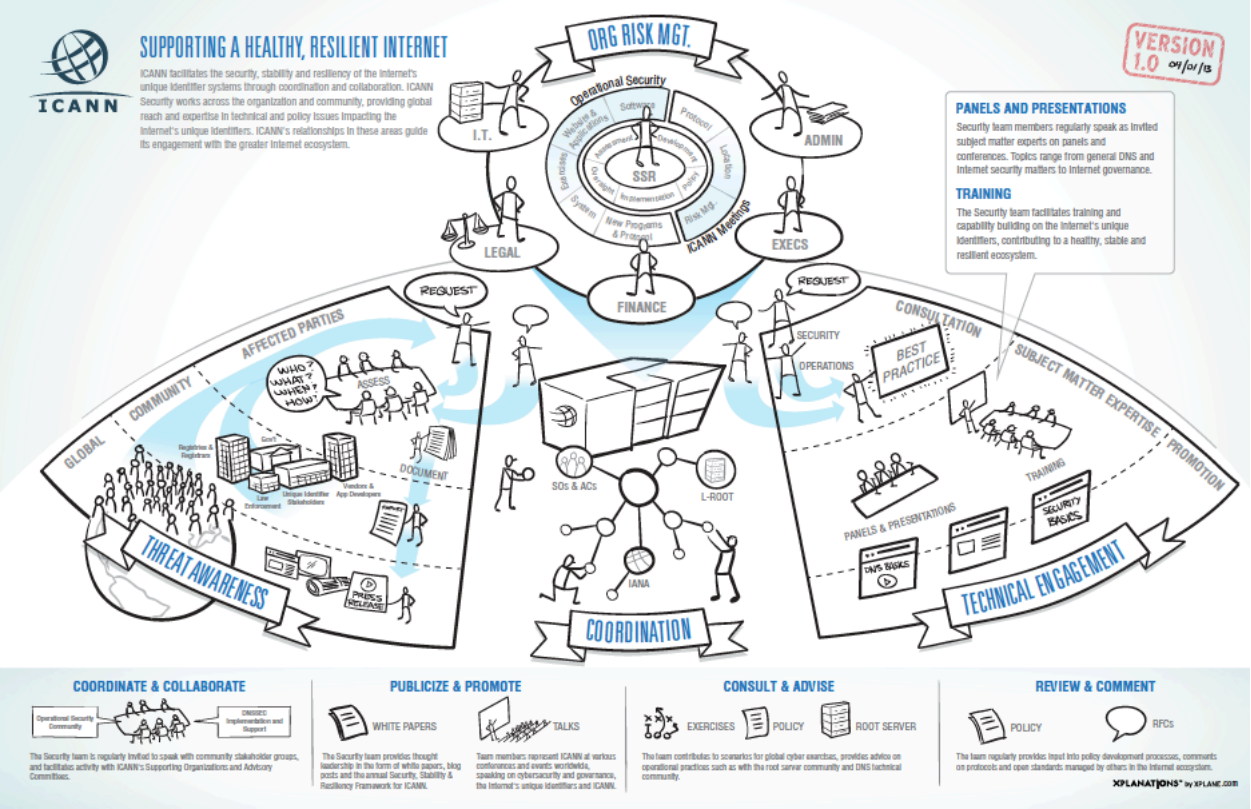


Рис. 7 — Графическое представление деятельности отдела безопасности ICANN

На рисунке показаны основные функции ICANN по обеспечению безопасности, включающие поддержку управления организационными рисками, распространение информации об угрозах для уникальных идентификаторов Интернета, сотрудничество и согласование действий с партнерами из интернет-сообщества, а также предоставление помощи специалистов в конкретной предметной области при решении технических вопросов, в том числе проведение обучения, интеллектуальное лидерство и предоставление консультаций по техническим проблемам и вопросам политики. (Примечание: эта схема является рабочим документом, который будет пересмотрен к началу конференции ICANN в Пекине).

Место обеспечения безопасности, стабильности и отказоустойчивости в сфере деятельности ICANN

Обеспечение безопасности в ICANN может рассматриваться в качестве:

- одной из основных ценностей, провозглашенных в «Подтверждении обязательств»;
- одного из четырех ключевых направлений стратегического плана;
- общей тематической области для всей организации;
- одного из отделов в структуре ICANN;
- необходимой составляющей проектов и мероприятий.

Отдел безопасности ICANN — это коллектив сотрудников, находящихся в различных географических точках по всему миру и обладающих большим опытом решения технических проблем и вопросов политики, связанных с уникальными идентификаторами Интернета. Отдел безопасности выполняет как внутренние, так и внешние функции, действуя в рамках организации и сообщества и способствуя реализации миссии ICANN по сохранению и повышению устойчивости работы, надежности и глобальной оперативной совместимости Интернета. Эта деятельность не всегда носит очевидный или публичный характер, но, тем не менее, очень важна для ICANN и для соблюдения ею своих обязательств. Отдел безопасности служит мостом, соединяющим операторов DNS, техническое сообщество, правоохранительные органы, сообщество и группы заинтересованных сторон, занимающиеся вопросами операционной безопасности.

Сотрудники отдела безопасности ICANN

На момент публикации данного документа в состав отдела безопасности входят:

- Джефф Мосс (Jeff Moss) — вице-президент и начальник отдела безопасности (руководитель отдела и член команды высших руководителей ICANN; специалист по техническому взаимодействию, часто выступающий с докладами по вопросам безопасности Интернета)
- Джефф Бикерс (Geoff Bickers) — директор по мерам безопасности (корпоративные программы безопасности, безопасность конференций, безопасность объектов и персонала ICANN, связь с отделом ИТ ICANN)
- Джон Крейн (John Crain) — старший директор по безопасности, стабильности и отказоустойчивости (техническое взаимодействие, лидерство в распространении информации об угрозах и мониторинге, представитель по вопросам коневых серверов в совете DNS-OARC)
- Патрик Джонс (Patrick Jones) — старший директор по безопасности (координация коллективной деятельности, член команды высших руководителей ICANN, представитель в отделе международного взаимодействия с заинтересованными сторонами ICANN, участие в управлении Интернетом)

- Ричард Лэмб (Richard Lamb) — старший руководитель программы, DNSSEC (техническое взаимодействие по вопросам внедрения и обучения DNSSEC, сотрудничество с сообществом по управлению политикой в отношении DNSSEC и методам развертывания DNSSEC)
- Дэйв Пищителло (Dave Piscitello) — старший технолог по вопросам безопасности (техническое взаимодействие, обучение и интеллектуальное лидерство, связи с правоохранительными органами и сообществом специалистов по операционной безопасности, член группы исполнительного руководства в рамках «Инициативы стран Содружества по борьбе с киберпреступностью»)
- Шон Пауэлл (Sean Powell) — инженер по вопросам информационной безопасности (безопасность деятельности организации; сетевая и информационная безопасность; сотрудничество с отделом ИТ ICANN и поддержка деятельности директора по безопасности)

Фото 1 — Джефф Мосс (Jeff Moss) на Российском форуме управления Интернетом (IGF)

Фото 2 — Джон Крейн (John Crain), Рик Лэмб (Rick Lamb) (ICANN) и Ревил Вудинг (Revil Wooding) (PCH) на конференции Карибской группы сетевых операторов CaribNOG 3

Фото 3 — Патрик Джонс (Patrick Jones) на диалоге по кибербезопасности Организации американских государств (ОАГ), декабрь 2012 г.

Фото 4 — Дэйв Пищителло (Dave Piscitello) выступает в Обществе международного уголовного права (ICLN), Гаага, декабрь 2012 г.

Критерии взаимодействия

В феврале 2012 года отдел безопасности формализовал свои критерии безопасности для разъяснительной работы и расширения участия. Эти критерии повлияли на работу и других отделов ICANN и предназначены в качестве ориентиров, которым отдел безопасности ICANN и исполнительное руководство будут следовать в рамках различных видов сотрудничества и деятельности сообщества, поддерживаемых отделом безопасности.

Таблица 1 —Критерии безопасности для разъяснительной работы и расширения участия

Виды мероприятий	Примеры
Открытые конференции ICANN	Конференции ICANN в Пекине, Дурбане, Буэнос-Айресе
Внутренние собрания ICANN	Совещания руководства, отдела безопасности, семинары Правления, обучение персонала, бюджет и др.
Встречи, связанные с вопросами деятельности ICANN/IANA/корневой сервер «L»/DNSSEC и др.	IETF, DNS-OARC, RIPE NCC, ГОС, ККБС, ККСКС и др.
Встречи, в которых ICANN участвует как партнер по борьбе с глобальными угрозами и смягчению их последствий	РГБФ, MAAWG, конференции Интерпола по теневой экономике, учения по деятельности в киберпространстве, ОАГ

Виды мероприятий	Примеры
Техническое взаимодействие — обучение и наращивание потенциала	Обучение реагированию на нападения и чрезвычайные происшествия (ПРНЧП), безопасность деятельности реестров, DNSSEC, правоохранительные органы и правительства, Инициатива стран Содружества по борьбе с киберпреступностью
Симпозиумы, конференции для приглашенных предприятий среднего и малого бизнеса, непрерывное образование	SATIN, Симпозиум по БСО, конференция Security Confab, RSA, BlackHat, FIRST, ICLN
Участие в экосистеме, модели многостороннего сотрудничества	IGF и региональные IGF, РАЕН, ОЭСР, Форум ВВИО, Панарабская кибербезопасность, CTU

Критерии взаимодействия	✓
Способствует ли мероприятие выполнению одной из стратегических задач ICANN	1. Сопровождение и поддержание работоспособности DNS 2. Улучшение управления рисками и отказоустойчивости DNS 3. Содействие широкому внедрению DNSSEC 4. Расширение международного сотрудничества в области DNS 5. Улучшение мер реагирования на происшествия в сфере безопасности DNS
Вписывается ли мероприятие в рамки одной из следующих сфер:	1. Эксплуатационная/организационная 2. Сотрудничество 3. Техническое взаимодействие
Проводится ли мероприятие в поддержку партнерских отношений, меморандума о взаимопонимании или связей с заинтересованными сторонами?	
Способствует ли мероприятие сохранению и упрочению репутации ICANN как организации?	
Как часто проводится мероприятие?	
Можно ли встретиться в месте проведения мероприятия или рядом с ним с другими заинтересованными сторонами?	Кто еще присутствует на мероприятии?
Как это вписывается в бюджет?	Проводится ли мероприятие для поддержки другого отдела?

В рамках новой матричной структуры отдел безопасности обеспечивает поддержку отдела международного взаимодействия с заинтересованными сторонами (GSE) ICANN и других ее отделов. Ниже приводятся примеры мероприятий и событий, поддерживаемых отделом безопасности ICANN:

- Конференции IETF в Ванкувере и Атланте
- Конференции X-Con, CNNIC и CONAC в Китае
- BlackHat и DefCon в Лас-Вегасе, Абу-Даби и Амстердаме
- Группа экспертов ООН по географическим наименованиям/конференция ООН по стандартизации географических наименований в Нью-Йорке
- Конференция Интерпола по теневой экономике в Лионе, Франция
- Конференция по реестрам СНГ в Будве, Черногория
- Тренинг по DNS совместно с Агентством по борьбе с особо опасной организованной преступностью и Управлением добросовестной конкуренции в Лондоне, Великобритания
- Тренинг по DNSSEC в Колумбии совместно с .CO; в Перу совместно с .PE и в Гонконге совместно с Центром ресурсов для запуска сетей
- Тренинг по наращиванию потенциала DNS совместно с LACTLD на Сен-Мартине и в Парагвае
- Конференция Азиатско-тихоокеанского союза электросвязи в Макао
- MENOG в Иордании
- LACNIC/LACNOG в Уругвае
- Тренинг по DNS с участием Европола
- MAAWG, РГБФ, RIPE NCC и DNS-OARC
- Запуск CICTE ОАГ своей CyberLab для проведения учений
- APNIC 34
- ION в Мумбаи и Interop
- Участие в обсуждениях посредством удаленного доступа, например, на IGF Карибского бассейна в Сент-Люсии в августе 2012 г. и конференции по ИКТ в Непале в феврале 2013 г.

Одним из основных направлений работы отдела безопасности в сфере технического взаимодействия является проведение тренингов по DNS по просьбе сообщества. Отдел разработал программу обучения, включающую следующие модули:

- Основы DNS (включая обзор участия в деятельности ICANN)
- Программа реагирования на атаки и чрезвычайные происшествия для операторов ДВУ

- Тренинг по DNS для правоохранительных органов и сообщества специалистов по операционной безопасности
- Тренинг по DNSSEC
- Курс по безопасности деятельности реестров

ICANN совместно с Центром ресурсов для запуска сетей (http://nsrc.org/), работающим на базе университета Орегона, регулярно проводит мероприятия по техническому взаимодействию с региональными организациями ДВУ, университетами и операторами со всего мира. Партнерами ICANN в этой обучающей деятельности также выступают AfTLD, APTLD и LACTLD.

Новое в международной деятельности

На мировой арене в 2013 ФГ наблюдалась значительная активность. ICANN подписала принципы обеспечения отказоустойчивости кибернетических систем Мирового экономического форума http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf и приняла участие в его мероприятиях в Давосе, Швейцария, и Вашингтоне, округ Колумбия, в 2012 и 2013 гг.

В июне 2012 г. в рамках конференции ICANN в Праге ICANN организовал семинар группы «Инициатива стран Содружества по борьбе с киберпреступностью» (CCI). В ноябре 2012 г. Дейв Пищителло из отдела безопасности ICANN был назначен в группу исполнительного руководства CCI (http://blog.icann.org/2012/11/icann-security-team-members-appointed-to-lead-roles-in-global-community-initiatives/).

ICANN обеспечивала проведение тренингов по DNSSEC в Латинской Америке и в странах Карибского бассейна (Тринидад, Колумбия Чили, Перу и Парагвай).

В июле Министерство торговли США объявило о заключении с ICANN договора на выполнение функций IANA, http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann. 9 июля 2012 г. ICANN опубликовала отредактированный вариант своего предложения по договору о функциях IANA: https://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm. Срок исполнения — с 1 октября 2012 года по 30 сентября 2015 г., с возможностью продления договора еще на два двухлетних периода при общем семилетнем сроке действия.

В июле 2012 г. ICANN участвовала в конференции по кибербезопасности ОАГ в Уругвае и в диалоге по кибербезопасности ОАГ 13 декабря 2012 г. в Вашингтоне. http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-465/12.

В августе 2012 г. IAB, IEEE-SA, IETF, интернет-общество и W3C запустили проект Open Stand (http://open-stand.org/), который призван стать открытой моделью для коллективной демократической разработки стандартов инновации и оперативной совместимости. Эта инициатива соответствует заявленным ICANN принципам многостороннего сотрудничества с использованием демократической процедуры принятия решений на основе консенсуса.

ICANN участвовала в работе 3-го Совета по безопасности, надежности и оперативной совместимости средств связи (CSRIC III), проведенного Федеральной комиссией связи США

(FCC). В сентябре 2012 г. Рабочая группа 4 опубликовала отчет по Передовому опыту обеспечения безопасности сетей (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf). ICANN также принимала участие в деятельности Рабочей группы 3 по DNSSEC и Рабочей группы 7 по кодексу поведения поставщиков интернет-услуг в отношении борьбы с ботнетами.

В октябре 2012 г. ICANN принимала участие в Будапештской конференции по киберпространству (http://www.cyberbudapest2012.hu/), организованной в продолжение Лондонской конференции 2011 г. (https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement).

В октябре 2012 г. ICANN совместно с Рабочей группой по вопросам борьбы с фишингом (РГБФ) провела 4-й Глобальный симпозиум по БСО DNS на конференции eCOS в Пуэрто-Рико (http://docs.apwg.org/events/2012_ecrime.html).

В октябре 2012 г. ОЭСР опубликовала анализ стратегий национальной кибербезопасности, отметив поддержку многостороннего диалога по кибербезопасности в нескольких документах по национальной стратегии. См. следующий документ ОЭСР (от 2012 г.): «Поворотная точка в формировании политики кибербезопасности: анализ нового поколения стратегий национальной кибербезопасности для интернет-экономики» («Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy»), документы ОЭСР по вопросам цифровой экономики, № 211, публикация ОЭСР. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

В ноябре 2012 г. ICANN была хорошо представлена на 7-ом Форуме управления Интернетом в Баку, Азербайджан (http://blog.icann.org/2012/10/icann-at-internet-governance-forum-2012-2/), где безопасность Интернета была одной из основных тем для обсуждения (http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/927-igf-2012). Кроме того, представители ICANN присутствовали на мероприятиях региональных IGF в Латинской Америке и странах Карибского бассейна, в России, Объединенных Арабских Эмиратах и в Соединенных Штатах.

В декабре 2012 г. генеральный директор ICANN Фади Шехаде выступил на открытии Всемирной конференции по международной связи в Дубае (http://www.itu.int/en/wcit-12/Pages/speech-chehade.aspx). В феврале 2013 г. ICANN участвовала в подготовке неофициальной группы экспертов для предстоящего женевского Всемирного форума по политике в области телекоммуникаций в мае 2013 г.

В декабре 2012 г. ICANN принимала участие в работе Панарабского пункта наблюдения за кибербезопасностью, где поделилась с участниками информацией о своей роли и сфере компетенции по обеспечению безопасности, стабильности и отказоустойчивости. Кроме того, ICANN участвовала в конференции сети международного уголовного права в Гааге, Нидерланды, и помогала Европолу организовать обучение по DNS в связи с открытием нового Европейского центра по борьбе с киберпреступлениями (EC3).

В январе 2013 г. отдел безопасности ICANN опубликовал концептуальный документ под названием «Важность оценки косвенного ущерба перед запросом на конфискацию домена» http://blog.icann.org/2013/01/the-value-of-assessing-collateral-damage-before-

requesting-a-domain-seizure/. Этот документ выпущен в продолжение концептуального документа «Конфискация и отмена регистрации доменных имен», опубликованного в марте 2012 г. http://blog.icann.org/2012/03/thought-paper-on-domain-seizures-and-takedowns/. Этот связано с документом ККБС SAC 056 «Консультативное заключение о последствиях блокирования контента через систему доменных имен», http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf, опубликованным в октябре 2012 г.

ICANN следила за разработкой стратегии ЕС по кибербезопасности (январь 2013 г.), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security и указа президента США о кибербезопасности (февраль 2013 г.), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. Оба документа отражают растущий интерес к созданию механизмов обмена информацией и сотрудничества в ответ на угрозы кибербезопасности.

Основные события, связанные с мировым Интернетом, происходившие к моменту публикации данного документа, включают:

- APRICOT 2013 (Конференция Азиатско-Тихоокеанского региона по операционным технологиям) в Сингапуре, 19 февраля —1 марта 2013 г., http://www.apricot2013.net/.
- ВВИО+10, «К обществам, основанным на знаниях, во имя мира и развития» (организовано ЮНЕСКО) в Париже, 25-27 февраля 2013 г. http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/.
- Конференция Арабского форума управления Интернетом с многосторонним участием в Дубае, ОАЭ, и Африканского форума управления Интернетом с многосторонним участием в Аддис-Абебе, Эфиопия, http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm.
- IETF 86, Орландо, Флорида, 10-15 марта 2013 г., http://www.ietf.org/meeting/86/index.html.

Мероприятия на 2014 ФГ

Мероприятия ICANN на 2014 ФГ в поддержку здоровой, стабильной и отказоустойчивой экосистемы будут сосредоточены на следующем:

- Обеспечение наивысшего качества деятельности отделов IANA, ИТ и эксплуатации DNS
- Обеспечение технического взаимодействия (путем предоставления помощи специалистов в конкретной предметной области и интеллектуального лидерства, проведения тренингов по DNS и мероприятий по наращиванию потенциала — при необходимости совместно с партнерами)

- Стимулирование внедрения DNSSEC организациями, пользователями и операторами и повышение осведомленности о DNSSEC
- Выполнение рекомендаций группы проверки БСО
- Поддержка дальнейшего расширения возможностей корневого сервера «L», публикация данных и результатов измерений отделом эксплуатации DNS корпорации ICANN
- Подготовка Концепции управления рисками DNS и завершение цикла оценки
- Наращивание опыта в сфере управления рисками корпорации ICANN, позволяющего улучшить поддержку деятельности комитета Правления по рискам и растущих потребностей по управлению рисками ICANN как организации
- Поддержка создания новых центральных представительств в Сингапуре и Стамбуле и расширения возможностей отдела безопасности в этих городах во благо сообщества
- Выполнение функций ресурса для отдела международного взаимодействия с заинтересованными сторонами при проведении обсуждений по вопросам управления Интернетом и кибербезопасности в рамках представительства ICANN на конференциях и встречах
- Стимулирование и поддержка более широкого участия правоохранительных органов и сообщества специалистов по операционной безопасности в деятельности ICANN
- Взаимодействие с гражданским обществом по вопросам конфиденциальности и свободы слова, связанным с безопасностью уникальных идентификаторов и здоровьем экосистемы Интернета (расширение информационно-разъяснительной деятельности и привлечение участников экосистемы к работе над проблемами БСО)
- Укрепление внутренних сетей, ИТ-процессов и информационной безопасности ICANN
- Сотрудничество по проблемам DNS с техническим сообществом, операторами корневых серверов, разработчиками приложений и браузеров
- Поддержка деятельности отдела политики и отдела по связям с заинтересованными сторонами там, где это необходимо (при обсуждении вопросов, связанных с ККБС, ККСКС и БСО в ОП и КК)
- Обеспечение успешного проведения конференций ICANN в Дурбане, Буэнос-Айресе, Сингапуре и Лондоне

Для успешной реализации этих инициатив ICANN необходимо в 2014 году расширить отдел безопасности, включив в его состав сотрудников, обладающих дополнительным опытом и навыками. Это необходимо для удовлетворения потребностей сообщества и внедрения матричной структуры, осуществляемого в этом финансовом году. В бюджет и план работ на 2014 год, которые планируется опубликовать после пекинской конференции ICANN, будет включено обоснование предлагаемых на 2014 год мероприятий по БСО. Вышесказанное соответствует Рекомендациям по БСО номер 20 и 21, в которых указано, что ICANN должна повысить прозрачность информации об организационной структуре и бюджетных средствах, связанных с реализацией концепции обеспечения БСО, а также что ICANN должна создать процедуру с более четкой структурой для демонстрации связи решений по организационной структуре и бюджетным средствам с концепцией обеспечения БСО.

Приложения

Приложение А — Отслеживание процесса выполнения рекомендаций ГП БСО

В настоящем разделе более подробно излагаются подходы к реализации 28 рекомендаций группы проверки БСО в соответствии с 4 сферами управления.

Констатация цели — круг обязанностей и миссия ICANN

Рекомендация ГП БСО	Выполнение и состояние
№ 1 — ICANN должна опубликовать единое, четкое и последовательное заявление о своем круге обязанностей по обеспечению БСО и выполнении ограниченной технической миссии.	В период май-сентябрь 2012 г. состоялось общественное обсуждение проекта заявления [ссылка: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm]. Проект заявления был пересмотрен 4 октября 2012 г. [http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct2012-en.pdf]. Обновленная версия представлена в Концепции БСО на 2014 ФГ.
№ 2 — Определение и пути реализации круга обязанностей ICANN по обеспечению БСО и выполнению ограниченной технической миссии должны подлежать пересмотру для сохранения консенсуса и содействия получению предложений от сообщества.	Обновленное заявление о функциях и круге обязанностей будет пересмотрено следующей ГП БСО в 2015 г.
№ 24 — ICANN должна четко сформулировать устав, функции и обязанности своей службы безопасности.	**Выполнено** путем обновления страницы отдела безопасности [ссылка: https://www.icann.org/security] 4 октября 2012 г. и опубликования Концепции БСО на 2013 ФГ. Функции и обязанности будут дополнительно уточняться при внедрении в 2013 г. новой структуры управления.
№ 18 — ICANN должна проводить ежегодный оперативный анализ прогресса в реализации концепции обеспечения БСО и включать этот анализ в состав компонентов концепции обеспечения БСО на следующий год.	**Выполнено** в рамках концепции обеспечения БСО на 2013 ФГ и будет осуществляться ежегодно. Информация для отслеживания хода выполнения этой задачи будет добавлена на новую страницу информационной панели отдела безопасности на веб-сайте ICANN.

Совершенствование деятельности — задачи

Рекомендация ГП БСО	Выполнение и состояние
№ 7 — ICANN должна развивать текущую Концепцию обеспечения БСО, сформулировав четкий список задач и определив приоритет своих инициатив и видов деятельности в	Для приведения задач и инициатив ICANN в соответствие с ежегодной концепцией обеспечения БСО, а также в качестве основы для разработки бюджета на 2014 ФГ, плана работ и следующего стратегического плана ICANN будет использоваться новая структура управления. ICANN уже работает над приведением своих задач и деятельности в

Рекомендация ГП БСО	Выполнение и состояние
соответствии с этими задачами.	соответствие с этой структурой.
№ 8 — ICANN должна продолжить уточнение задач своего стратегического плана, в частности, задачи сопровождения и поддержания работоспособности DNS. Необходимо обеспечить полную согласованность концепции и стратегического плана.	Это связано с подготовкой следующего стратегического плана. Необходимо привести задачи и деятельность в стратегическом плане в соответствие с ежегодной концепцией обеспечения БСО и рекомендациями группы проверки БСО.

Совершенствование деятельности — прозрачность

Рекомендация ГП БСО	Выполнение и состояние
№ 17 — ICANN должна создать внутренний процесс с более четкой структурой для демонстрации связи различных видов деятельности и инициатив с конкретными стратегическими целями, задачами и приоритетами концепции обеспечения БСО.	Структура управления уже принесла пользу при выполнении этой рекомендации, создав механизм реализации внутреннего процесса, который будет демонстрировать, как деятельность и инициативы ICANN в области БСО связаны с конкретными стратегическими целями, задачами и приоритетами. Дополнительная информация об этом процессе станет доступна сообществу через MyICANN и веб-сайт ICANN в 2013 г. в период между конференциями в Пекине и Дурбане.
№ 20 — ICANN должна повысить прозрачность информации об организационной структуре и бюджетных средствах, связанных с реализацией концепции обеспечения БСО и выполнением функций, связанных с БСО.	Это будет реализовано в рамках подготовки концепции обеспечения БСО на 2014 ФГ, а также плана работ и бюджета на 2014 ФГ. Для выполнения данной рекомендации также будет использоваться новая страница информационной панели отдела безопасности.

Совершенствование деятельности — структура

Рекомендация ГП БСО	Выполнение и состояние
№ 21 — ICANN должна создать внутренний процесс с более четкой структурой для демонстрации связи решений по организационной структуре и бюджетным средствам с концепцией обеспечения БСО, включая лежащий в основе анализ издержек и выгод.	ICANN будет использовать работу по управлению как структурно оформленный процесс определения организационных и бюджетных решений и приведения их в соответствие с деятельностью по БСО в ежегодной Концепции. Это будет реализовано в плане работ и бюджете на 2014 ФГ.

Совершенствование деятельности — стандарты и соответствие требованиям

Рекомендация ГП БСО	Выполнение и состояние
№ 9 — ICANN должна оценить возможности сертификации своих эксплуатационных обязанностей на соответствие общепринятым международным стандартам (например, ITIL, ISO и SAS-70). ICANN должна опубликовать четкий оперативный план такой сертификации.	Внедрение корпорацией ICANN системы DNSSEC в корневой зоне достигло этапа сертификации SysTrust [ссылка: https://www.iana.org/dnssec/systrust иhttps://cert.webtrust.org/icann.html]. Другие процедуры сертификации осуществляются под руководством входящих в состав ICANN отдела выполнения функций IANA, отдела ИТ и оперативной группы DNS, при поддержке со стороны отдела безопасности.
№ 10 — ICANN должна продолжать усилия, направленные на обеспечение выполнения сторонами своих договорных обязательств, а также предоставить адекватные ресурсы для выполнения этой функции. ICANN также должна разработать и внедрить имеющий более четкую структуру процесс мониторинга проблем соблюдения обязательств и проведения расследований.	Выполнение этой рекомендации осуществляется под руководством отдела обеспечения соблюдения обязательств ICANN, а также путем реализации рекомендаций группы проверки WHOIS.

Совершенствование деятельности — новые ДВУ

Рекомендация ГП БСО	Выполнение и состояние
№ 11 — ICANN должна доработать и внедрить меры по обеспечению успеха новых рДВУ и ускоренного ввода ИДИ, которые прямо относятся к задачам программ в сфере БСО, включая средства измерения эффективности механизмов предотвращения злоупотреблений в системе доменных имен.	Персонал изучает все аспекты выполнения этой рекомендации. По мнению отдела безопасности, для ее полного выполнения потребуется сотрудничество сообщества и персонала. Поскольку это связано с проверкой конкуренции, доверия потребителей и возможностей потребительского выбора, а также с показателями для новых рДВУ и нДВУ с ИДИ, делегированных в рамках процедуры ускоренного ввода нДВУ с ИДИ, ожидается взаимодействие с заинтересованными сторонами из всех частей сообщества. В центре данной рекомендации находятся механизмы, относящиеся к снижению количества злоупотреблений доменными именами. Персонал обеспечивает поддержку усилий консультативных комитетов и сообщества по разработке количественных показателей злоупотреблений.

Рекомендация ГП БСО	Выполнение и состояние
№ 22 — ICANN должна публиковать, постоянно контролировать и обновлять документацию по организационной структуре и бюджетным ресурсам, необходимым для управления различными аспектами БСО параллельно с вводом новых рДВУ.	Это связано с рекомендацией № 21 (решения по организационной структуре и бюджетным средствам), а также с разработкой системы мониторинга последствий ввода новых рДВУ.

Совершенствование деятельности — управление рисками и смягчение угроз

Рекомендация ГП БСО	Выполнение и состояние
№ 25 — ICANN должна ввести механизмы выявления долгосрочных рисков и стратегических факторов в рамках своей концепции управления рисками	Это осуществляется в настоящее время и связано с завершением подготовки концепции управления рисками согласно рекомендации № 26.
№ 26 — ICANN должна уделить первостепенное внимание своевременному завершению подготовки концепции управления рисками.	Это осуществляется в настоящее время. ICANN наняла компанию Westlake Governance для помощи в реализации проекта разработки концепции управления рисками DNS. Westlake провела в Торонто открытое заседание, в скором времени представит проект концепции и проведет брифинг по элементам концепции на конференции ICANN в Пекине.
№ 27 — Концепция управления рисками ICANN должна носить комплексный характер в пределах круга обязанностей по обеспечению БСО и выполнению ограниченных миссий	Концепция управления рисками будет приведена в соответствие с деятельностью ICANN в поддержку своей технической миссии и сообщества. В этих пределах она будет носить комплексный характер и сопровождаться концепцией, подготовленной согласно рекомендации № 26.
№ 15 — ICANN должна действовать как координатор ответственного раскрытия и распространения информации об угрозах DNS и методах их смягчения.	В настоящее время отдел безопасности ICANN разрабатывает проект процедуры согласованного раскрытия информации. Персонал корпорации сотрудничает с операторами и авторитетными лицами в сообществе специалистов по безопасности, в части устранения угроз безопасности DNS и разработки методов их смягчения. Это связано с рекомендацией № 28.

Рекомендация ГП БСО	Выполнение и состояние
№ 28 — ICANN не должна прекращать своего активного участия в обнаружении и устранении угроз, а также своего участия в усилиях по распространению информации об угрозах и происшествиях.	Эта рекомендация поддерживает продолжение работы ICANN, включающей мониторинг корневой зоны, обнаружение и смягчение угроз, относящихся к деятельности ICANN по эксплуатации DNS, а также угроз и происшествий в DNS в целом.

Интернационализация — терминология и взаимосвязи

Рекомендация ГП БСО	Выполнение и состояние
№ 3 — После опубликования согласованного заявления о своем круге обязанностей по обеспечению БСО и выполнении ограниченной технической миссии ICANN должна использовать во всех материалах единообразную терминологию и описания из данного заявления.	Отдел безопасности будет работать в масштабе всей организации над использованием в документах ICANN единообразной терминологии и описаний, относящихся к роли и кругу обязанностей ICANN по обеспечению БСО. Первым шагом станет проведение обучения с участием персонала ICANN, а затем — проведение интернет-семинара для членов сообщества. Мы также будем использовать эту терминологию и описания в презентациях ICANN и во время встреч.
№ 4 — ICANN должна документально оформить и четко определить характер своих взаимоотношений в сфере БСО в рамках сообщества ICANN с целью создания единой отправной точки для понимания взаимосвязи между организациями.	Работа над документальным оформлением и определением этих взаимоотношений уже началась. Визуализация функций отдела безопасности ICANN будет использоваться для сопоставления их с функциями координации и сотрудничества, осведомленностью об угрозах и сферами технического сотрудничества.
№ 5 — ICANN должна использовать определение своих взаимоотношений в сфере БСО для сохранения эффективных рабочих схем и продемонстрировать, как эти взаимоотношения используются для достижения каждой цели в сфере БСО.	Отдел безопасности вместе с отделом международного взаимодействия с заинтересованными сторонами ICANN будет работать над сохранением и улучшением эффективных рабочих схем и взаимосвязей. Отдел безопасности установил связи с правоохранительными органами и сообществами специалистов по операционной безопасности во всем мире и уже провел тренинги, в частности, в Чешской Республике, Франции, Нидерландах, Великобритании и США.

Интернационализация — разъяснительная деятельность и сотрудничество

Рекомендация ГП БСО	Выполнение и состояние
№ 14 — ICANN должна обеспечить неуклонное развитие своей информационно-разъяснительной деятельности в сфере БСО для сохранения ее актуальности, своевременности и целесообразности.	Информационно-разъяснительная деятельность расширена и будет ежегодно пересматриваться. Сотрудники отдела безопасности одновременно выполняют функцию обслуживания отдела международного взаимодействия с заинтересованными сторонами ICANN как эксперты в предметной области и функцию разъяснительной деятельности и сотрудничества с сообществом в сфере БСО.
№ 16 — ICANN не должна прекращать своих усилий, направленных на расширение участия сообщества и его вклада в процесс разработки концепции обеспечения БСО. ICANN также должна внедрить процесс более регулярного получения предложений со стороны других участников экосистемы.	Информационно-разъяснительная деятельность и соответствующие процессы расширены и будут ежегодно пересматриваться. Результатом текущего сотрудничества отдела безопасности с сообществами специалистов по операционной безопасности, такими как РГБФ и MAAWG , стало участие членов этих сообществ в работе ККБС. Посредством своего взаимодействия с ICLN и CCI отдел безопасности демонстрирует важность многостороннего участия в решении вопросов кибербезопасности. Это связано с рекомендациями № 4, 5 и 14. Отдел безопасности, по запросу заинтересованных сторон, обеспечивает поддержку множества инициатив по наращиванию возможностей, таких как обучение DNSSEC, обучение реагированию на атаки и непредвиденные ситуации в нДВУ, обучение правоохранительных органов, разъяснительная деятельность на встречах групп операторов сетей, в том числе таких, как CaribNOG, MENOG.

Развитие модели многостороннего сотрудничества

Рекомендация ГП БСО	Выполнение и состояние
№ 6 — ICANN должна опубликовать документ, подробно описывающий функции и обязанности ККБС и ККСКС, чтобы четко разграничить деятельность этих двух групп.	Для выполнения этой рекомендации потребуется совместная работа сообщества и персонала корпорации. Для удобства отслеживания процесса реализации данной рекомендации она разделена на подразделы 6A [ККБС] и 6B [ККСКС]. 6A — роли и обязанности ККБС определены в рабочих процедурах ККБС. ККБС в настоящее время изучает свои рабочие процедуры на 2013 год и также заинтересован в их согласовании с функциями и обязанностями ККСКС. 6B — роль и обязанности ККСКС находятся в стадии разработки после окончания общественного обсуждения предлагаемых поправок к Уставу ICANN в отношении ККСКС. См. http://www.icann.org/en/news/public-comment/bylaws-03jan13-en.htm.

Рекомендация ГП БСО	Выполнение и состояние
№ 12 — ICANN должна работать с сообществом над выявлением передовых практических методов в области БСО и поддерживать внедрение таких методов через договоры, соглашения и меморандумы о взаимопонимании, а также другие механизмы.	Реализация рекомендации номер 12 потребует совместных усилий сообщества и персонала ICANN. Дальнейшее обсуждение этого вопроса будет происходить на конференции ICANN в Пекине в группе экспертов по безопасности DNS с участием технической рабочей группы ОПНИ по передовым неконтрактным методам. Отдел безопасности совместно с Комитетом по вопросам политики Интернета РГБФ опубликовал рекомендации по защите веб-приложений, участвовал в разработке информационных ресурсов по вопросам безопасности (посредством мероприятий SANS Securethehuman.org и NCA Stop.Think.Connect). Страница текущего периода общественного обсуждения исправленного варианта соглашения о реестре нового рДВУ (см. http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm) содержит дополнительную формулировку в разделе о передовых методах.
№ 13 — ICANN должна поощрять разработку и опубликование всеми организациями поддержки передовых практических методов в сфере БСО для своих членов.	Эта рекомендация будет включать совместную работу сообщества и персонала ICANN через ОПА, ОПНИ и ОПРИ по выявлению соответствующих передовых методов, связанных с уникальными идентификаторами.
№ 19 — ICANN должна внедрить процесс, позволяющий сообществу отслеживать реализацию концепции обеспечения БСО. Информация должна предоставляться с достаточной степенью детализации, позволяющей сообществу следить за выполнением корпорацией ICANN своих обязательств в отношении БСО	Отдел безопасности скоро предоставит на своей странице доступ к панели мониторинга, отображающей состояние инициатив, относящихся к концепции обеспечения БСО и деятельности ICANN в сфере БСО, и позволяющей отслеживать это состояние.

Рекомендация ГП БСО	Выполнение и состояние
№ 23 — ICANN должна предоставить надлежащие ресурсы рабочим группам и консультативным комитетам, занимающимся вопросами БСО, в соответствии с возложенными на них обязанностями. ICANN также должна в обязательном порядке создать такие условия, в которых рабочие группы и консультативные комитеты смогут принимать объективные решения без какого-либо внутреннего или внешнего давления.	В настоящее время персонал составляет перечень деятельности [23A] в существующих рабочих группах и консультативных комитетах (ККБС и ККСКС), занимающихся вопросами БСО. Затем будет подготовлено описание или документация по процессу подготовки бюджета для предоставления ОП и КК возможности направлять свои предложения [23B]. 23C будет описывать стандартный этап рабочего процесса, демонстрирующий объективность принятия решений ОП/КК/рабочей группой.

SSR RT Recommendations Tracking – February 2013

Recommendation	FY 13 T1	T2	T3	FY 14 T1	T2	T3	FY 15 T1	T2	T3
Rec 1 – Clear statement of ICANN's SSR role and remit	Published	Revise	Update						
Rec 2 – Role & remit review in 2015								Review	Publish
Rec 3 – Use consistent terminology	Develop	Ongoing							
Rec 4 – Document & define SSR relationships		Develop	Publish						
Rec 5 – Use SSR relationships for effective working	Ongoing	Ongoing	Ongoing						
Rec 6 – Roles for SSAC (6A) & RSSAC (6B)		Publish							
Rec 7 – Build from SSR Framework, clear objectives & priorities	Develop	Publish	Expected Complete	Reporting					
Rec 8 - Strategic Plan & SSR Framework alignment		Publish	Refine						
Rec 9 – Assess certification options, publish roadmap		Develop	Publish						
Rec 10 – Process for monitoring compliance & investigations (see Whois RT Implementation)		Whois RT Recs							
Rec 11 – Measures for success in nTLD & IDN FT re SSR			Develop	Publish			AoC CCR		
Rec 12 – w/Community, SSR-related best practices	Engage	Discuss							
Rec 13 – Encourage SOs/SGs to develop & publish SSR-related best practices			Expected Complete						
Rec 14 – Evolving SSR outreach		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 15 – Facilitate responsible disclosure of threats		Draft	Ongoing	X					
Rec 16 – Outreach w community; process for input		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 17 – Mapping activities to SSR Framework		Publish	X	Reporting					
Rec 18 (Implemented w FY 13 SSR Framework) – Annual review of SSR Framework	Complete								
Rec 19 – Dashboard for SSR Framework			Publish	Reporting					
Rec 20 – Transparency on SSR budget			Publish	ongoing					
Rec 21 – Show how budget & op decisions relate to SSR			Publish						
Rec 22 – Documenting mgmt. of SSR issues with operational readiness from introduction of nTLDs		Develop	Publish						
Rec 23 – Appropriate resources for SSR-related WGs & ACs		FY 14 Budget	Budget approx						
Rec 24 (Implemented w FY 13 SSR Framework) – Define Security team roles	Complete								
Rec 25 – DNS Risk Management Framework	Consultant	Draft	Publish	Assess	work	work	Review		
Rec 26 – Prioritizing completion of DNS RMF		Publish	Approv						
Rec 27 – DNS RMF covers IANA, L-root, other functions				Assess	work	work	Review		
Rec 28 – Active engagement in threat detection & mitigation	Underway	X							

Рис. 8 — Отслеживание выполнения рекомендаций ГП БСО

Приложение B — Отчет о состоянии на 2013 ФГ

Задача в целом	Программа/инициатива	Состояние
Сотрудничество в области глобальной безопасности	Участие широкого сообщества, бизнеса, научного и технического сообществ и правоохранительных органов в решении вопросов безопасности DNS	Проведение в октябре 2012 года 4-го Всемирного симпозиума по БСО DNS совместно с РГБФ на конференции eCOS в Пуэрто-Рико
		Семинары группы «Инициатива стран Содружества по борьбе с киберпреступностью» в рамках конференций ICANN в Коста-Рике и Праге, встречи Руководящей группы CCI и EMG
		BlackHat/Defcon в июле 2012 г.
		Форум управления Интернетом и региональные мероприятия Форума
		Выступление перед постоянной группой коммерческих пользователей в Вашингтоне, округ Колумбия, и участие в подготовке информационного бюллетеня этой группы для конференции ICANN в Торонто
Сотрудничество	Дальнейшая поддержка принятия средств измерения и учета показателей работы DNS, таких как программа ATLAS реестра RIPE NCC	Помощь реестру RIPE NCC в дальнейшем внедрении узлов ATLAS и анализе данных. https://atlas.ripe.net/
	Автоматизация корневой зоны	Системе управления корневой зоной (RZM), используемой IANA совместно с NTIA и Verisign, в августе 2012 г. исполнился один год (см. http://blog.icann.org/2012/08/rzm-is-one-year-old/). Отдел IANA работает над дополнительными процедурами обеспечения безопасности, такими как система безопасного уведомления. См. http://www.icann.org/en/news/public-comment/iana-secure-notification-12dec12-en.htm.
	Техническое обучение с участием правоохранительных органов и сообщества специалистов по операционной безопасности	Отдел безопасности принимал представителей правоохранительных органов на конференциях ICANN в Праге и в Торонто, а также проводил тренинг по DNS для Европола в Нидерландах и для SOCA, OFT и лондонской полиции в Великобритании.
	Безопасность и стабильность Консультативный комитет	Сотрудничество с ККБС при проведении семинаров по DNSSEC на конференциях ICANN; рабочие комиссии, отчеты и рекомендации ККБС. В 2013 ФГ ККБС была проделана значительная работа.

Задача в целом	Программа/инициатива	Состояние
	Поддержка РГ по вопросам анализа безопасности и стабильности DNS	В августе 2012 г. DSSA завершила отчет по этапу 1. http://www.icann.org/en/news/public-comment/dssa-phase-1-report-14aug12-en.htm. Группа DSSA снова соберется во время конференции ICANN в Пекине. Кроме того, ICANN привлекла компанию Westlake Governance для разработки концепции управления рисками DNS.
	Техническая эволюция WHOIS	В феврале 2013 г. ICANN объявила о создании группы экспертов по справочным службам рДВУ (https://www.icann.org/en/news/announcements/announcement-14feb13-en.htm). В октябре 2012 г., ICANN объявила о привлечении CNNIC к работе над внедрением сервера RESTful WHOIS с открытым кодом http://blog.icann.org/2012/10/cnnic-selected-to-implement-an-open-source-restful-whois-server/.
	Разработка политики — злоупотребления при регистрации; Соглашение об аккредитации регистраторов	ICANN проводит период общественного обсуждения предварительного отчета по универсальности отчетности, https://www.icann.org/en/news/public-comment/uofr-20feb13-en.htm. Данный отчет явился результатом решения Совета ОПРИ в ответ на информацию рабочей группы по вопросам политики борьбы со злоупотреблениями при регистрации. Продолжаются переговоры по условиям Соглашения об аккредитации регистраторов. 7 февраля 2013 г. генеральный директор Фади Шехаде представил обновленную информацию по этой проблеме, http://blog.icann.org/2013/02/registrar-accreditation-agreement-negotiation-session/.
	DNSSEC — рабочая комиссия ККБС по смене ключей	Рабочая комиссия ККБС по смене ключей корневой зоны продолжает свою деятельность в 2013 году. Дополнительная информация будет предоставлена на конференции ICANN в Пекине. Успешные церемонии смены ключей были проведены в Кулпепере, Вирджиния, и Эль-Сегундо, Калифорния.
	DNSSEC — аудит SysTrust	Сертификат SysTrust по DNSSEC находится по ссылке https://www.iana.org/dnssec/systrust.
	Тренинг по DNSSEC с участием сообщества	ICANN обеспечила проведение тренингов по DNSSEC в Колумбии, Перу, Парагвае, Российской Федерации, Чили и планирует провести тренинги в Ливане (март 2013 г.) и в Тунисе (апрель 2013 г.).
	Отказоустойчивость корневого сервера «L»	ICANN поддерживает рост количества и распространение экземпляров корневого сервера «L» во всем мире. В частности, было объявлено о создании партнерства с целью внедрения экземпляров корневого сервера «L» в Африке — с AfriNIC, в Латинской Америке и странах Карибского бассейна — с LACNIC, в Бразилии с — CGI.Br, в Корее — с Корейским управлением по делам Интернета и безопасности (KISA), а также в других местах.

Задача в целом	Программа/инициатива	Состояние
Программы корпоративной безопасности	Повышение безопасности внутренних сетей и процедур ICANN	Отдел безопасности совместно с отделом ИТ работает над укреплением внутренних сетей ICANN. Отдел обеспечивал проведение тренинга по программе SANS для сотрудников отдела ИТ, а также тренинг по основам безопасности для сотрудников ICANN в Лос-Анджелесе и Брюсселе.
	Улучшение непрерывности деятельности и проведение внутренних учений	Отдел безопасности обеспечивал проведение учений по отказоустойчивости корневых серверов и поддержку внутренней системы обмена информацией.
	Безопасность конференций — оценка рисков, безопасность участников	Проведение оценки рисков в местах проведения конференций ICANN, обеспечение работы медицинских и аварийных служб непосредственно на месте проведения конференций ICANN (ISOS)
В масштабах всей организации	Поддержка работы с новыми рДВУ	Помощь отделу по работе с новыми рДВУ в отношении процедур определения приоритета методом жеребьевки; процессы проверки
		Помощь домену .SE в анализе системы проверки перед делегированием http://www.icann.org/en/news/announcements/announcement-21dec12-en.htm.
	Обеспечение соблюдения договорных обязательств	Отдел соблюдения договорных обязательств продолжил свое развитие в 2013 году, опубликовав план аудита (см. http://www.icann.org/en/resources/compliance/audits)
	Программа ИДИ	Участие в конференциях ГЭГНООН/КООНСГН (UNGEGN/UNCSGN) в Нью-Йорке в июле и августе 2012 года в штаб-квартире ООН, продолжающаяся работа по программе вариантных ИДИ.
	Управление корпоративными рисками	ICANN наняла компанию Westlake Governance для разработки концепции управления рисками DNS. Дополнительная информация о том, что сделано Westlake на данном этапе, будет предоставлена на конференции ICANN в Пекине.

Работа по техническому взаимодействию, выполняемая отделом безопасности ICANN, является результатом совместных усилий. Мы делаем это на благо широкого сообщества. Очень приятно получать письма со словами поддержки нашей работы, но это не означает, что нам просто нравится коллекционировать лестные для нас отзывы. Приведенные ниже письма являются примером поддержки со стороны сообщества, которую ICANN получила в 2013 ФГ за работу по обеспечению безопасности.

COMNET
Foundation for ICT Development

www.comnet.org.mt

ICANN Security Team

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

2nd July 2012

Re: Commonwealth Cybercrime Initiative

Dear ICANN Security Team,

We would like to express our gratitude and thanks for providing the Commonwealth Cybercrime Initiative the opportunity to host another workshop at the ICANN Meeting in Prague. The Event in Costa Rica was a big success and to follow with another space in Prague was excellent as it provided continuity. We sincerely appreciate the time and resources that ICANN has invested to provide a platform for the Initiative to raise its profile amongst the ICANN community.

Our Prague workshop resulted in two expressions of interest in the CCI from two governments in Africa and we also had excellent additions to our expert resource repository. We are already working on translating these expressions of interest into meaningful activity on the ground.

We are especially grateful of Mr Dave Piscitello's contributions in his capacity as ICANN representative on the CCI Steering Group. Mr Piscitello's involvement, in a very short time resulted in very tangible achievements for the Initiative.

ICANN's support of the Commonwealth Cybercrime Initiative has proven invaluable and we look forward to the opportunity to present the CCI at the next ICANN meeting in Canada if scheduling allows.

Thank you once again, and we look forward to our continued collaboration.

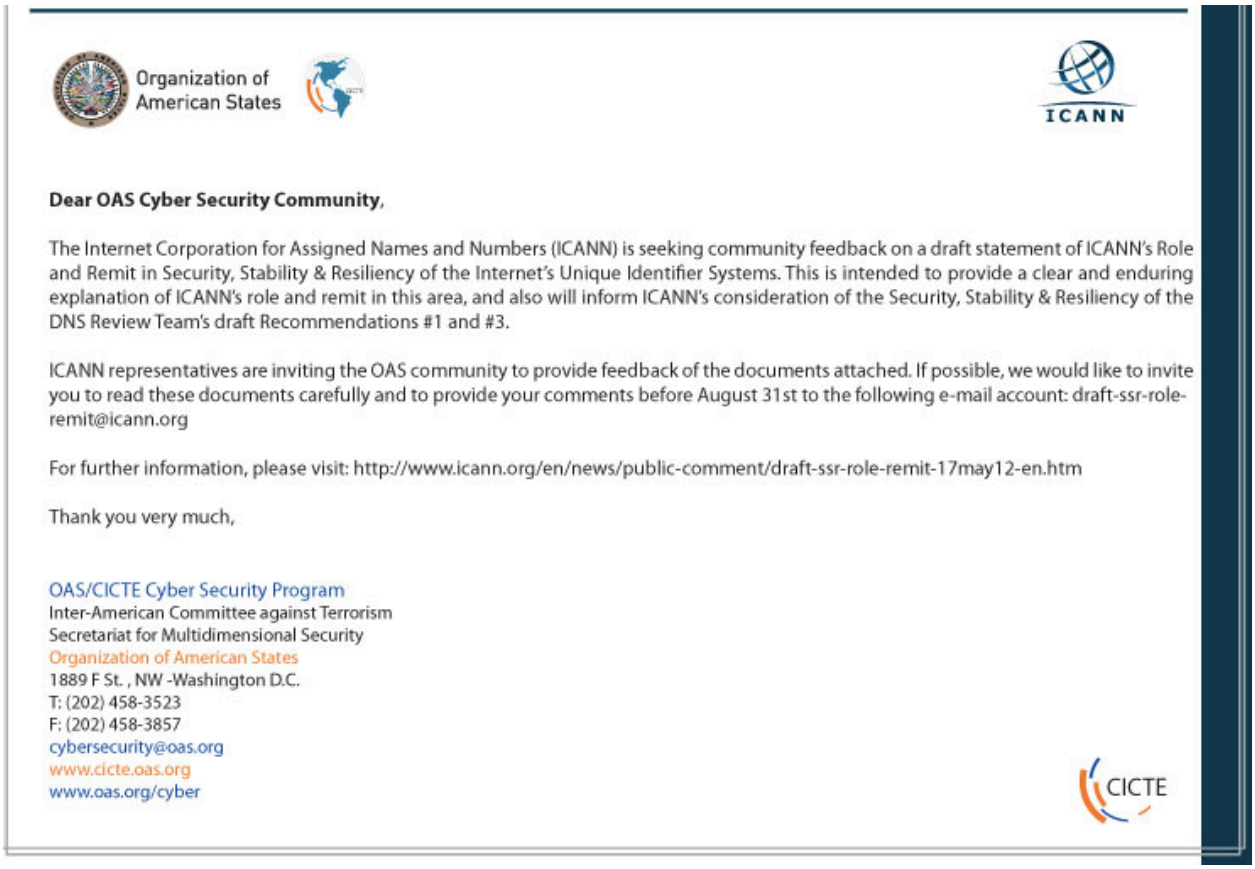
Yours,

Joseph V. Tabone

Chairman CCI Secretariat

Alfir, Reggie Miller Street, Gzira, GZR 1541, Malta | t: (356) 2132 3393 | f: (356) 2132 3390 | e: info@comnet.org.mt

Приложение C — Письмо ICANN от COMNET



Organization of American States

ICANN

Dear OAS Cyber Security Community,

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. This is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also will inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

ICANN representatives are inviting the OAS community to provide feedback of the documents attached. If possible, we would like to invite you to read these documents carefully and to provide your comments before August 31st to the following e-mail account: draft-ssr-role-remit@icann.org

For further information, please visit: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm

Thank you very much,

OAS/CICTE Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States
1889 F St. , NW -Washington D.C.
T: (202) 458-3523
F: (202) 458-3857
cybersecurity@oas.org
www.cicte.oas.org
www.oas.org/cyber

CICTE

Приложение D — Запрос на общественное обсуждение в адрес сообщества ОАГ

CARIBBEAN TELECOMMUNICATIONS UNION
3rd Floor, Victoria Park Suites, 14-17 Victoria Square, Port of Spain, Trinidad & Tobago, W.I.
Tel: (868)627 0281/0347 Fax: (868) 623 1623 E-Mail: ctunion@ctu.int Website: www.ctu.int

7th September, 2012

Mr. Patrick Jones
Senior Manager, Security
Internet Corporation for Assigned Names and Numbers (ICANN)
1101 New York Ave
New York Avenue
Washington DC 20005
USA

Dear Mr. Jones,

Expression of Appreciation

On behalf of the Caribbean Telecommunications Union (CTU), I would like to express our sincere appreciation to you for participating in the CTU's 8th Caribbean Internet Governance Forum, which took place from the 29th to 30th August, 2012 at the Bay Gardens Hotel, Castries, St. Lucia.

Thank you for your presentation on "DNSSEC, Collaboration and Training" which was well received by the audience.

I take this opportunity to re-affirm the CTU's commitment to Caribbean ICT development and look forward to an ongoing partnership with ICANN in supporting Caribbean countries as they seek to leverage the power of ICT for social and economic development.

Sincerely,

Bernadette Lewis
SECRETARY GENERAL

Приложение E — Письмо ICANN от Телекоммуникационного союза стран Карибского бассейна

Europol Unclassified – Basic Protection Level

The Hague, 3 January 2013

Ref: 647233

Dr Stephen D. Crocker
Internet Corporation for Assigned Names and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Dear Dr Crocker, Dear Steve!

Dave Piscitello of ICANN visited us in The Hague on 12 December. The purpose of this meeting was for Dave to be informed on the development of the new European Cybercrime Centre (EC3), ourselves to be aware of ICANN cooperation with law enforcement and all of us to see how this could specifically work between ICANN and the EC3.

We were all pleased by the constructive dialogue and positive outcomes of the meeting. There appear clear opportunities for the EC3 to play the role of facilitator with ICANN for MS law enforcement, both with respect to their views on internet governance and in training to improve investigative capabilities. We will be in contact with Dave over the specifics concerning this in the coming weeks.

The EC3 is very appreciative of this initiative between our two organisations and hope that you can lend your full support to it. Thank you very much.

Yours sincerely,

Troels Oerting
Assistant Director
Head of European Cybercrime Centre (EC3)

EDOC#647233

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

Приложение F — Письмо ICANN от EC3