# План повышения безопасности, стабильности и отказоустойчивости Интернета

ОДОБРЕННЫЙ ПРОЕКТ – 16 мая 2009 г.

# Содержание

# Сводное резюме

Интернет представляет собой успешную экосистему, в которой разнообразные субъекты организованы на основе сотрудничества, направленного на стимулирование общения, творчества и торговли в глобальной среде. Возможность взаимодействия в рамках этой среды зависит от функционирования и координации систем уникальных идентификаторов Интернета.[1] ICANN и операторы этих систем осознают, что поддержание и повышение безопасности, стабильности и отказоустойчивости этих систем является ключевым элементом их сотруднических отношений.

В стратегическом плане ICANN на 2009-2012 гг. (www.icann.org/en/strategic-plan/strategic-plan-2009-2012-09feb09-en.pdf) говорится: «Безопасность, стабильность и отказоустойчивость останутся наивысшим приоритетом и ICANN будет эффективно сотрудничать с другими заинтересованными сторонами над укреплением защиты, безопасности и стабильности Интернета, уделяя особое внимание решению задач корпорации по защите безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета». В стратегическом плане определён ряд задач по всему спектру ответственности ICANN в отношении безопасности, стабильности и отказоустойчивости. В стратегическом плане поднимаются вопросы безопасности, стабильности и отказоустойчивости согласно второму Приоритету – Повышение безопасности, стабильности и отказоустойчивости при выделении и присвоении уникальных Интернет-идентификаторов. Второй Приоритет гласит: Безопасная, стабильная и отказоустойчивая работа системы уникальных Интернет идентификаторов является ключевой часть задачи ICANN. В свете увеличения количества нападений с применением новейших технологий и злонамеренного поведения ICANN и её сообщество должны продолжать улучшать отказоустойчивость DNS и укреплять её возможности по борьбе с такими атаками. В свете расширения разновидностей атак и злонамеренного поведения ICANN должна проводить работу со всеми заинтересованными сторонами, направленную на разъяснение роли ICANN и поиск решений проблем, выходящих за рамки миссии любой отдельно взятой организации. Принципиальной задачей данного приоритетного направления является обеспечение стабильной работы системы

[1] Согласно уставу ICANN корпорация координирует распределение и назначение трёх комплектов уникальных идентификаторов для Интернета: доменных имён, формирующих систему, называемую DNS; адресов Интернет-протокола (IP, произносится «ай-пи») и номеров автономной системы (AC); а также портов протоколов и номеров параметров.

уникальной идентификации Интернета в течение срока действия плана.

Во втором приоритете стратегического плана указаны следующие конкретные цели.

A. Предоставить план для обсуждения, определяющий роль ICANN в обеспечении безопасности, стабильности и отказоустойчивости Интернета; определить подходящих партнёров и начать совместную работу. Определить роль ICANN таким образом, чтобы чётко прояснить сферу деятельности, затраты и результаты, и запустить процесс, целью которого является заключение соглашения между сообществом и Советом в 2009 году. Эффективно сотрудничать с партнёрами для осуществления многосторонних подходов и программ, способствующих глобальной безопасности, стабильности и отказоустойчивости Интернета. Показатели данных программ буду установлены к концу 2009 г., а их предварительная оценка проведена к середине 2010 г.

B. Обеспечить механизмы, дающие пользователям возможность проверять подлинность Интернет-идентификаторов, публикуемых ICANN, и непосредственно участвовать в технических работах по обеспечению более безопасных систем распределения имен и адресов Интернета. В частности, ICANN приложит все усилия для сотрудничества с ключевыми заинтересованными сторонами в обеспечение использования DNSSEC подписей корневой зоны DNS к концу 2009 года и способствования внедрению КОИр для повышения безопасности и стабильности адресной системы.

C. Реализовывать программы, направленные на разъяснение вопросов, связанных с рисками, и укрепление безопасности и отказоустойчивости организаций, связанных с сообществом ДВУ. Эти программы включают сотрудничество с партнёрами по формулированию результативных подходов к обмену передовым опытом в сообществе к концу 2009 года и реализации текущих региональных образовательных программ для этого сообщества в рамках сроков осуществления данного плана.

D. Работать с заинтересованными сторонами в сообществе ICANN для организации постоянного сотрудничества в целях укрепления безопасности и отказоустойчивости DNS перед всем спектром угроз в рамках сроков осуществления данного плана. ICANN продолжит сотрудничество с партнёрами по разработке подходов к измерению операционных рисков для DNS и её пользователей к середине 2010 г.

В плане ICANN по повышению безопасности, стабильности и отказоустойчивости содержится документ, на необходимость которого указывается в задаче A, подробно описывающий конкретную роль ICANN в обеспечении безопасности, стабильности и отказоустойчивости, предоставляющий обзор инициатив ICANN в этой области и сообщающий подробности запланированных мер по увеличению вклада корпорации в течение следующего года. Первый вариант плана предполагается в качестве основы роли ICANN и её сообщества и для формирования структуру организации усилий по обеспечению безопасности, стабильности и отказоустойчивости. В плане не предусмотрен ввод новых значительных ролей или программ для ICANN в этой области.

## Роль ICANN

Процессы формулирования политик и программ ICANN, включая относящиеся к безопасности, стабильности и отказоустойчивости, осуществляются при участии ряда разнообразных субъектов, на основе консенсуса и в соответствии с уставом корпорации.

- Роль ICANN должна в первую очередь относиться к ключевым задачам корпорации, связанным с системами уникальных идентификаторов.
- ICANN не выполняет роли полицейского Интернета по оперативному противодействию криминальной деятельности.
- ICANN не участвует в использовании Интернета для кибер-разведки и кибервойны.
- ICANN не участвует в определении составляющих противозаконного содержимого в Интернете.
- Роль ICANN включает участие в деятельности широкого Интернет-сообщества по борьбе со злоупотреблениями систем уникальных идентификаторов. Такая деятельность подразумевает сотрудничество с правительственными структурами по борьбе со злоумышленными преступлениями, связанными со злоупотреблениями упомянутых систем, и их защите.

## Программы ICANN по обеспечению безопасности, стабильности и отказоустойчивости

- ICANN несёт ответственность за деятельность Агентства по распределению номеров Интернета (IANA). Обеспечение безопасного, стабильного и отказоустойчивого функционирования корневой зоны DNS было и остаётся основным приоритетом.

- ICANN поддерживает усилия сообщества системы доменных имён (DNS) и адресного сообщества по укреплению основ системы в части безопасности, стабильности и отказоустойчивости. Эти усилия включают поддержку разработки и внедрения протоколов и вспомогательных технологий по аутентификации Интернет-имён и номеров.
- ICANN обеспечивает и способствует осуществлению мероприятий в сфере безопасности, стабильности и отказоустойчивости, проводимых реестрами DNS, регистраторами и прочими участниками сообщества.
- ICANN несёт ответственность за безопасную, стабильную и отказоустойчивую деятельность своих собственных активов и служб.
- ICANN принимает участие в широких форумах и мероприятиях, направленных на обеспечение безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета.

## Планы по повышению безопасности, стабильности и отказоустойчивости

В ходе рабочего года 2009–2010 ICANN планирует реализовать нижеизложенные программы и инициативы. В приложении A указаны конкретные цели, участники, результаты и ресурсные требования программ и мероприятий.

- ***Деятельность IANA*** – в соответствии со стратегическим планом ICANN на 2009-2012 гг., ICANN следует обеспечить операционную готовность к внедрению DNSSEC для авторитетной корневой зоны, в также сотрудничать с Интернет-сообществом по устранению препятствий для принятий DNSSEC. ICANN выражает готовность, желание и способность обеспечить подписание корня. Согласно предложению от сентября 2008 г. текущие и планируемые усилия ICANN описываются в разделах 5.1.1.3 и 6.1.1.1. Прочие инициативы включают улучшение управления корневой зоной посредством автоматизации; улучшение методов аутентификации сообщений, обмениваемых с менеджерами ДВУ.
- ***Операции корневого сервера DNS*** – продолжение стремления к взаимному признанию ролей и ответственностей и инициирование добровольных усилий, направленных на осуществление планирования и проведение учений на случай чрезвычайных происшествий.
- ***Реестры рДВУ*** – обеспечить дальнейшую безопасность деятельности в ходе оценки заявок на новые родовые домены верхнего уровня (рДВУ) и интернациональные

доменные имена (ИДИ). ICANN продолжит дорабатывать план бесперебойной работы реестров рДВУ и тестировать систему ответственного хранения данных.

- ***Реестры нДВУ*** – ICANN активизирует сотрудничество с национальными доменами верхнего уровня (нДВУ) по доработке совместной программы планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП), введённой в сотрудничестве с организацией поддержки национальных имён (ОПНИ) и региональными ассоциациями доменов верхнего уровня (ДВУ).
- ***Выполнение договорных обязательств*** – ICANN продолжит расширять масштабы деятельности по обеспечению выполнения договорных обязательств, связанных с рДВУ, и начнёт проведение аудиторских проверок субподрядчиков в рамках исполнения поправок к соглашению об аккредитации регистраторов от 9 марта и определение потенциальной вовлечённости субподрядчиков в злоумышленную деятельность для принятия исправительных мер.
- ***Реагирование на предумышленное злоупотребление DNS*** – ICANN продолжит развивать сотруднические усилия и способствовать обмену информацией для обеспечения эффективного реагирования на злоумышленное поведение, связанное со злоупотреблением DNS.
- ***Внутренние операции ICANN по обеспечению безопасности и непрерывности*** – ICANN продолжит реализацию программ безопасности в рамках общих программ управления корпоративным риском, управления кризисными ситуациями и программ непрерывности деятельности. Основное внимание будет уделено устройству крепкого фундамента задокументированных планов и вспомогательных процедур.
- ***Обеспечение повсеместного участия и сотрудничества*** – ICANN будет расширять партнёрские отношения с такими организациями, как Комиссия по технологиям Интернета (Internet Engineering Task Force, IETF), Общество Интернета (Internet Society, ISOC), региональные Интернет-реестры (РИР) и группы операторов сетей (ГОС), операционного, аналитического и исследовательского центра DNS (DNS-ОАИЦ; DNS Operations, Analysis and Research Center, DNS-OARC). ICANN также будет принимать участие в межнациональных диалогах, направленных на расширение понимания трудностей с сфере безопасности, стабильности и отказоустойчивости, стоящих перед экосистемой Интернета, и способов решения этих трудностей при участии большого количества субъектов.

# 1. Цель и обзор

1.1 В данном плане широкому ряду субъектов обрисовывается, как ICANN будет участвовать во всемирных усилиях по решению трудностей, стоящих перед Интернетом в области безопасности, стабильности и отказоустойчивости, уделяя особое внимание основной задаче корпорации, связанной с уникальными идентификаторами Интернета. В плане разъясняются роли и рамки ICANN, определяющие способ её вовлечённости в эту сферу; обозреваются существующие программы ICANN этой направленности; и приводятся подробности запланированных мероприятий и выделенных ресурсов на следующий рабочий год. План состоит из семи разделов и приложения:

- Раздел 1: Цель и обзор
- Раздел 2: Трудности и возможности
- Раздел 3: Роль ICANN
- Раздел 4: Участие ICANN в усилиях в сфере безопасности, стабильности и отказоустойчивости
- Раздел 5: Продолжающиеся программы ICANN, связанные с безопасностью, стабильностью и отказоустойчивостью
- Раздел 6: Планы ICANN по повышению безопасности, стабильности и отказоустойчивости на FY10
- Раздел 7: Заключение
- Приложение A: Цели, участники, вехи и результаты и ресурсные требования программы ICANN по обеспечению безопасности, стабильности и отказоустойчивости на FY 10

1.2 Как указано в сводном резюме, данный план развивает видение и задачи, описанные в стратегическом плане ICANN на 2009-2012 гг. Первый вариант плана предполагается в качестве основы роли ICANN и её сообщества и для формирования структуру организации усилий по обеспечению безопасности, стабильности и отказоустойчивости. В плане не предусмотрен ввод новых значительных ролей или программ для ICANN в этой области. План будет ежегодно обновляться в соответствии с циклами стратегического и оперативного планирования ICANN.

# 2. Трудности и возможности

2.1 Динамичной Интернет-среде угрожает рост интенсивности злоумышленных преступлений различного рода, включая интенсивное участие криминальных организаций в мошенничестве, вымогательстве и прочей незаконной деятельности онлайн, а также рост числа нападений, вызывающих отказ в обслуживании и прочей деструктивной деятельности, осуществляемой через Интернет. Деятельность в Интернете всё в большей мере отражает полный спектр человеческих мотиваций и поведений. В прошлом такая деятельность отражала открытую природу Интернета, принёсшую ему успех, позволила осуществлять передовые нововведения и способствовала общению, творчеству и торговле в глобальной среде. Однако открытость принесла с собой уязвимость. К примеру, растут случаи использования возможностей для «обмана» или «отравления» процесса работы DNS для направления ничего не подозревающих пользователей по неправильным компьютерным адресам. Схожим образом, продолжает расти и количество случаев захвата систем маршрутизации, регистрации адресов и регистрации номеров автономной системы (НАС). Нападения, вызывающие отказ в обслуживании (DoS) способны нарушить работу пользователей самого различного рода. За последние несколько лет растущую обеспокоенность выражают все Интернет-субъекты – пользователи; предприятия; суверенные государства; равно как и организации, вовлечённые в обсуждения, связанные с Интернетом, и более широкая информационная общественность. Усилия по решению этих трудностей должны быть также направлены против рисков для безопасности и стабильности, проистекающих из введения новых инструментов контроля, которыми могут воспользоваться в своих интересах преступники, или конструкций сетей, усложняющих обеспечение стабильности.

2.2 ICANN будет бороться с угрозами для безопасности, стабильности и отказоустойчивости Интернета в рамках своей сферы ответственности. В статье I устава ICANN указано, что задача ICANN заключается в «общем координировании глобальной Интернет-системы уникальных идентификаторов и обеспечении стабильной и безопасной работы систем уникальных идентификаторов Интернета». Программы и деятельность ICANN в этой области сосредоточены на достижении трёх основных характеристик систем уникальных идентификаторов Интернета: безопасности, стабильности и отказоустойчивости. Безопасность определяется как способность защищать системы уникальных идентификаторов Интернета и предотвращать злоупотребление ими.

Стабильность – это способность обеспечивать ожидаемое функционирование системы и наличие в этом уверенности у пользователей систем уникальных идентификаторов. Отказоустойчивость представляет собой способность систем уникальных идентификаторов эффективно реагировать и отвечать на злоумышленные нападения и прочие виды деструктивной деятельности, а также восстанавливаться от них. ICANN сотрудничает с ответственными сторонами, представляющими различные элементы систем уникальных идентификаторов для обеспечения ответственности за адекватную реализацию её политик и договорных обязательств. Будучи организацией, которой движут самые различные заинтересованные стороны, ICANN обеспечивает наиболее эффективное использование имеющихся ресурсов сообщества в этой области, тесно сотрудничая с ключевыми субъектами и чётко определяя цели и параметры измерения эксплуатационных показателей при стратегическом, оперативном и финансовом планировании. План обеспечивает сообщество ориентирами на способы выполнения ICANN своих обязанностей. В приложении A к плану представлены подробности запланированных на 2010-й финансовый год (FY10) действий, вех и выделенных ресурсов. Большую долю внимания сотрудников отдела безопасности ICANN в FY10 будет занимать установление параметров для более объёмных программ, нацеленных на улучшение общей безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов.

# 3. Роль ICANN

3.1 Процессы формулирования политик и программ ICANN, включая относящиеся к безопасности, стабильности и отказоустойчивости, осуществляются при участии ряда разнообразных субъектов, на основе консенсуса и в соответствии с уставом корпорации. Ключевая задача ICANN заключается в обеспечении полисубъектного подхода к эффективному осуществлению функций IANA; установлении глобальных политик, обеспечивающих координацию DNS, адресацию через Интернет-протокол (IP) и назначения IP; а также по стимулированию конкуренции и выбора в среде рДВУ посредством системы контрактов с реестрами рДВУ и аккредитованными ICANN регистраторами.

3.2 Выполняя свою задачу, за последние десять лет ICANN сыграла определённую роль в повышении безопасности и стабильности систем уникальных идентификаторов Интернета. ICANN и соответствующие операторы систем уникальных идентификаторов признают и подтверждают, что поддержание и повышение безопасности и стабильности услуг является ключевым элементом их взаимоотношений. Данный принцип отражён в системе контрактов и соглашений между ICANN и операторами в зависимости от конкретной сущности отношений, ролей и взаимных обязанностей. Совместные усилия и их реализация обеспечивают необходимую уверенность в том, что уникальные идентификаторы и организации, предоставляющие их по всему миру, продолжат обеспечивать безопасность, стабильность и отказоустойчивость при помощи координированной, направленной на сотрудничество системы.

3.3 ICANN планирует продолжать вносить свой вклад по ряду направлений с целью обеспечения безопасности, стабильности и отказоустойчивости адресных и именных систем Интернета в свете развивающихся рисков и угроз. При этом корпорация обеспечит направленность своих усилий на выполнение своей ключевой задачи, связанной с системами уникальных идентификаторов Интернета. Корпорация не будет выступать в роли полицейского и не будет бороться с криминальной деятельностью отдельных злоумышленников на оперативном уровне. ICANN не занимается деятельностью и не вступает в диалоги, связанные с использованием Интернета для кибершпионажа и кибервойны. ICANN также не будет вступать в обсуждения составляющих незаконного содержимого, находящегося в Интернете или передаваемого через него. ICANN будет продолжать сотрудничать с широким

Интернет-сообществом в рамках ключевых форумов, связанных с борьбой против конкретных видов злонамеренных действий (например, фишинга и спама), использующих систему уникальных идентификаторов Интернета.

3.4 ICANN структурирует свою деятельность в сфере обеспечения безопасности, стабильности и отказоустойчивости посредством рассмотрения своей роли: как организации, несущей непосредственную ответственность; как организации, предоставляющей необходимые услуги или средства; как участника.

- ICANN несёт непосредственную ответственность за деятельность IANA и сотрудничает с министерством торговли США и фирмой VeriSign в области составления и распространения корневой зоны. Обеспечение безопасного, стабильного и отказоустойчивого функционирования корневой зоны DNS было и остаётся основным приоритетом. Кроме того, ICANN предоставляет ключевые услуги сообществу DNS и адресному сообществу, занимающимся аутентификацией Интернет-имён и номеров. ICANN продолжает отстаивать ту точку зрения, что важнейшим шагом по обеспечению безопасности DNS является внедрение расширений безопасности системы доменных имён (Domain Name System Security Extensions, DNSSEC), включая использование подписей в корневой зоне DNS. ICANN предложила подход, обеспечивающий продолжение бесперебойной работы механизма распределения корневой зоны DNS: ввод совместной ответственности ICANN, VeriSign, NTIA и операторов корневых серверов за работу DNSSEC. ICANN предложила гибкие решения, включающие промежуточный подход, способный перерасти в постоянное решение, и уже провела операционную подготовку для выполнения совей роли.. Прочие ключевые усилия сосредоточены на улучшении общесистемного понимания рисков, обеспечении реализации ключевой открытой инфраструктуры ресурсов (КОИр; Resource Public Key Infrastructure, rPKI), а также на сотрудничестве с партнёрами в области улучшения механизмов обеспечения безопасности и отказоустойчивости в рамках сообщества ДВУ.
- ICANN предоставляет услуги и ресурсы для деятельности по обеспечению безопасности, стабильности и отказоустойчивости, осуществляемой реестрами и регистраторами DNS. Характер ролей и обязанностей ICANN зависит от конкретных характеристик её взаимоотношений с этими ключевыми операторами. Наряду со своей сотруднической деятельностью ICANN заключила контракты

со всеми реестрами рДВУ и аккредитованными корпорацией регистраторами. Эти соглашения всё в возрастающей мере становятся механизмами для улучшения безопасности, стабильности и отказоустойчивости по всей DNS. Усилия ICANN по обеспечению соответствия и исполнения положений этих соглашений являются одним из ключевых элементов дальнейшего развития корпорации. В отношении нДВУ ICANN и операторы нДВУ выразили приверженность к дальнейшему повышению безопасности, стабильности и внутренней совместимости DNS на пользу местного и глобального Интернет-сообщества на основе равноправных взаимоотношений. Обмен информацией, взаимопомощь и расширение мощностей станут основными аспектами дальнейшего развития.

- ICANN принимает участие в деятельности Организации номерных ресурсов (ОНР; Numbering Resource Organization, NRO) и РИР, направляемой общим пониманием необходимости поддержания и повышения безопасности, стабильности и отказоустойчивости Интернета со стороны РИР и ICANN на благо местных и глобальных пользователей Интернета
- ICANN несёт прямую ответственность за безопасное, стабильное и отказоустойчивое функционирование своих собственных активов и служб при руководстве IANA и прочими координирующими функциями в качестве оператора L-корневого сервера DNS.
- Организации поддержки, консультативные комитеты и сотрудники ICANN являются ключевыми участниками более широких форумов и мероприятий, цели которых разнятся от повышения отказоустойчивости в свете деструктивных воздействий до совместных усилий, направленных на противодействие злоумышленникам в Интернете, распространяющим вредоносные программы и занимающимся фишингом с использованием систем уникальных идентификаторов Интернета. ICANN выполняет задачи общественного траста в свете её роли координатора систем уникальных координаторов Интернета и берёт на себя ведущую роль в решении трудностей, связанных с созданием безопасной, стабильной, отказоустойчивой экосистемы Интернета, которая при этом должна оставаться динамичной средой для глобального диалога, торговли и инноваций.

# 4. Участие ICANN в усилиях в сфере безопасности, стабильности и отказоустойчивости

Участие ICANN в сфере обеспечения безопасности, стабильности и отказоустойчивости включают деятельность самых различных сотрудников, организаций поддержки и консультативных комитетов корпорации. Среди ключевых участников можно перечислить следующих.

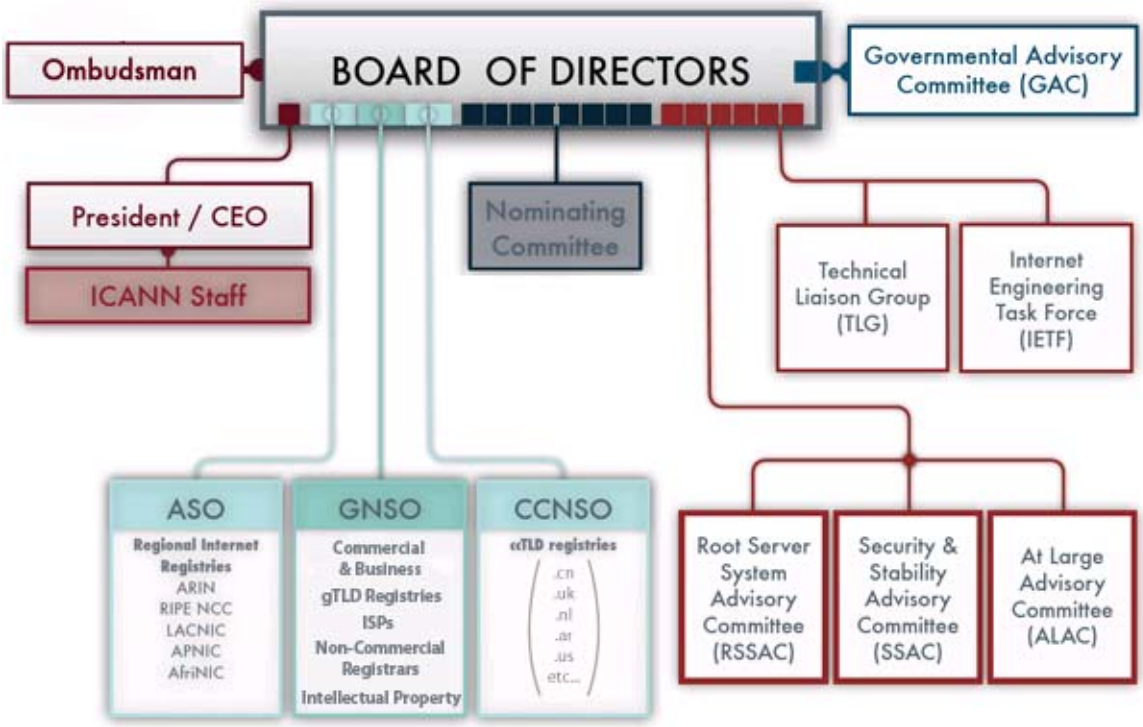
- ***Сотрудники IANA*** – ответственны за осуществление функций IANA, включая координацию корневой зоны DNS, эксплуатацию реестра .arpa, распределение пространства IP-адресов и регистрацию параметров протоколов. Сотрудники, ответственные за функции IANA, подготовили планы по внедрению DNSSEC на корневом уровне и в зонах DNS под управлением ICANN. Конкретные виды деятельности, связанные с обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.
- ***Сотрудники отделов услуг и выполнения договорных обязательств*** – ответственны за обеспечение координации и выполнения требований договоров реестрами рДВУ и аккредитованными ICANN регистраторами. Конкретные виды деятельности, связанные с обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.
- ***Сотрудники отдела политик*** – ответственны за содействие организациям поддержки и консультативным комитетам в осуществлении их деятельности, связанной с формулированием политик, включая политики рабочих групп сформированных организациями поддержки. Конкретные виды деятельности, связанные с обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.
- ***Сотрудники отдела глобальных партнёрств*** – ответственны за глобальное и региональное взаимодействие с субъектами ICANN с целью обеспечения полного глобального вовлечения корпорации в процессы эксплуатации и реализации. В этой связи деятельность ICANN, связанная с обеспечением безопасности, стабильности и отказоустойчивости, интегрируется в общий объём работ, выполняемых отделом глобальных партнёрств для корпорации.
- ***Сотрудники отделов корпоративных отношений и связи*** – ответственны за обеспечение эффективной популяризации планов и программ ICANN и представление организации и её

деятельности сообществу корпорации. Деятельность ICANN, связанная с обеспечением безопасности, стабильности и отказоустойчивости, интегрирована в её общую корпоративную программу связи.

- ***Сотрудники отдела безопасности*** – ответственны за каждодневное планирование и исполнение оперативных усилий ICANN, связанных с безопасностью, под руководством Правления и генерального директора ICANN, направленных на выполнение стратегических и оперативных планов корпорации. Отдел координирует усилия различных подразделений ICANN в обеспечение эффективного решения вопросов, касающихся безопасности, включая кибербезопасность и прочие форумы, связанные с безопасностью, стабильностью и отказоустойчивостью.
- ***Консультативный комитет по безопасности и стабильности (ККБС)*** – ККБС является консультативным комитетом ICANN, ответственным за определение для Правления и сообщества корпорации ключевых вопросов и трудностей, встающих перед ICANN при обеспечении безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета. Комитет проводит исследования по ключевым вопросам на основании запросов Правления ICANN и в рамках его описанного ниже мандата, а также сотрудничает с прочими организациями ICANN, как например, Организацией поддержки родовых имён (ОПНИ).
- ***Консультативный комитет системы корневого сервера (ККСКС)*** – ККСКС является консультативным комитетом ICANN по вопросам операционных потребностей корневых именных серверов; он анализирует и предоставляет консультации по вопросам безопасности системы корневого именного сервера и общих рабочих показателей, выносливости и надёжности системы.
- В более широком смысле, деятельность, связанная с безопасностью, стабильностью и отказоустойчивостью, осуществляется во всех организациях поддержки и консультативных комитетах ICANN, как описано ниже.

Сотрудники отдела безопасности ICANN несут общую ответственность за эффективное взаимодействие различных сегментов корпорации и реализацию интегрированного процесса планирования и отслеживания по указанным видам деятельности, а также за обеспечение синхронизации и интеграции работы различных отделов и субъектов. На Рисунке 1 отражены базовые организационные взаимоотношения в рамках структуры ICANN.

**Рисунок 1 – организационная структура ICANN**




# 5. Продолжающиеся программы ICANN, связанные с безопасностью, стабильностью и отказоустойчивостью

В данном разделе описываются крупные программы и мероприятия, реализованные ICANN и способствующие безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета, с указанием ключевым оперативных партнёров и продолжающихся усилий. Целью данного раздела плана является обеспечить базовое понимание широкого ряда мероприятий, проводимых ICANN, способствующих безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов. Привлечение к работе большинства старших сотрудников, организаций поддержки и консультативных комитетов позволяет ICANN эффективно исполнять свои обязанности в этой области. В данном разделе приводится предыстория и объяснение того, как

программы и мероприятия соотносятся со структурой ICANN и пересекаются со сторонними организациями.

Данный раздел составлен на основе структуры, установленной в разделе 3.4, начиная с ключевых функций DNS и адресной системы; работы с реестром ДВУ и сообществами регистраторов; взаимодействия с ОНР и РИР; программ корпоративной безопасности и непрерывности деятельности; деятельности организаций поддержки и консультативных комитетов, равно как и участия в обеспечении глобальной и региональной безопасности Интернета и участия в обеспечении глобальной и региональной Интернет-безопасности, стабильности и отказоустойчивости.

## 5.1 Безопасность, стабильность и отказоустойчивость DNS и адресной системы

### 5.1.1 Операции IANA

5.1.1.1 ICANN руководит функциями IANA в сотрудничестве с министерством торговли США, фирмой VeriSign, Комиссией по технологиям Интернета (IETF), региональными Интернет-реестрами (РИР) и операторами доменов верхнего уровня (ДВУ), как описано ниже. Эффективное осуществление этой деятельности является фундаментальным вкладом ICANN в стабильность и отказоустойчивость Интернета. Путём осуществления функций IANA ICANN координирует и управляет реестрами ключевых идентификаторов, обеспечивая существование глобального, внутренне совместимого Интернета.

5.1.1.2 Хотя Интернет знаменит тем, что является всемирной сетью свободной от централизованной координации, деятельность ключевых систем уникальных идентификаторов должна координироваться на мировом уровне – и именно в этой роли координатора выступает ICANN. В частности, через функции IANA ICANN выделяет и поддерживает уникальные коды и системы нумерации, используемые в технических стандартах («протоколах»), лежащих в основе Интернета. Различные виды деятельности IANA можно объединить в три широкие категории:

- ***Доменные имена*** – Через функции IANA ICANN управляет корнем DNS, доменами .int и .arpa, а также ресурсом практик интернациональных доменных имён (ИДИ).

Методики управления обеспечивают проверку каждого изменения в этих зонах на предмет воздействия на стабильность и безопасность конкретного домена верхнего уровня и корневой зоны в целом. Осуществление функций IANA также позволяет ICANN играть роль в обеспечении безопасности систем DNS и IP - адресов путём внедрения и поддержания «якорей доверия» в корневой зоне систем DNS и адресов, способных значительно укрепить целостность данных уникальных идентификаторов, а также целостность реакций в рамках системы DNS.

- ***Номерные ресурсы*** – Через функции IANA ICANN координирует глобальный резерв адресов IPv4 и IPv6, а также НАС, предоставляя их РИР. Процессы и процедуры, сформулированные в сообществах РИР в ходе их процессов разработки политики направляют координационную деятельность ICANN в рамках функций IANA. Открытые для участия процессы формулирования политик позволяют итоговым получателям ресурсов достигать всеобщий консенсус в отношении справедливости, предсказуемости и стабильности действий ICANN и РИР.
- ***Назначение протоколов*** – Через функции IANA ICANN осуществляет управление реестрами Интернет-протоколов и параметров совместно с IETF. ICANN применяет и поддерживает более 700 реестров протоколов и параметров в соответствии со стандартами, разработанными в ходе устоявшегося процесса согласования, заключающегося в публикации запросов о комментариях (ЗоК). В тесном сотрудничестве с IETF и авторами ЗоК персонал, ответственный за функции IANA, обеспечивает создание реестров посредством последовательных процессов и их поддержание в точном и готовом состоянии. Взаимоотношения между сотрудниками, ответственными за функции IANA, и IETF отражены в ЗоК 2860 и в соглашении об уровне услуг.

5.1.1.3 ICANN выступала в защиту необходимости внедрить DNSSEC на корневом уровне, в сентябре 2008 г. подала предложение в министерство торговли касательно роли функции IANA в подписании корневого уровня и провела подготовку в выполнению этой роли, а также к подписанию доменов .int и .arpa. Данные приготовления включают ведущееся с июня 2007 г. внедрение тестовой платформы для DNSSEC, сотрудничество с ДВУ и прочими операторами DNS относительно усилий по внедрению DNSSEC, приобретение технических навыков по

использованию криптологических методик в соответствии с действующими стандартами, и отражение усилий по внедрению DNSSEC в планах работ и бюджетах. ICANN сформировала специальную группу сотрудников, ответственную за эксплуатацию и обеспечение безопасности механизмов DNSSEC, включая подписание icann.org и iana.org. Наконец, для обеспечения дальнейшего продвижения DNSSEC ICANN организовала репозиторий IANA для отметок о доверии для доменов верхнего уровня (РОД-I) как способ обеспечить доступность ключей DNSSEC для ДВУ, уже внедривших её, для тех, кто ещё проводит внедрение DNSSEC.

5.1.1.4 Кроме того, ICANN сотрудничает с РИР и IETF по разработке технологии КОИр для ввода аутентификации назначенных ресурсов нумерации. Персонал, ответственный за функции IANA, сотрудничал с сообществом ДВУ при отслеживании внедрения общих средств в систему ДВУ, направленных на смягчение обнаруженной летом 2008 г. уязвимости к «отравлению» кэша DNS (см. доклад «Уязвимость кэша DNS к отравлению, 2008» по адресу http://www.iana.org/about/presentations/davies-cairo-vulnerability-081103.pdf). ICANN приложит все усилия для того, чтобы её программы и деятельность укрепляли безопасность, стабильность и отказоустойчивость процессов внесения изменений и дополнений в корневую зону и работу «якорей доверия» при запросах в рамках DNS, как описано ниже.

5.1.1.5 ICANN ежегодно предоставляет министерству торговли США план обеспечения безопасности информации, связанный с осуществлением функций IANA в соответствии с контрактом о функциях IANA, заключённым ICANN с министерством торговли, и в рамках её собственной корпоративной безопасности и планирования реагирования на чрезвычайные происшествия.

### 5.1.2 Операции корневого сервера DNS

5.1.2.1 ICANN сотрудничает с операторами корневых именных серверов в сфере безопасной и стабильной координации корневой зоны в обеспечение адекватного планирования на случай чрезвычайных происшествий и для поддержания чёткости процессов при внесении изменений в корневую зону. ICANN продолжит сотрудничество с операторами корневых именных серверов и прочими субъектами в сфере безопасной и стабильной координации системы корневого сервера.

ККСКС выступал в роли ключевого консультанта по вопросам воздействия на систему изменений в протоколах, таких, как добавление в корень записей IPv6.

5.1.2.2 ICANN продолжит работу по формализации отношений с операторами корневого именного сервера согласно обязательствам, взятым на ей себя в «Подтверждении обязанностей Правления ICANN в отношении управления частным сектором ICANN за 2006 г.» В 2008 г. ICANN заключила соглашение о взаимном распределении обязанностей с Консорциумом Интернет-систем относительно эксплуатации F-корня, закрепившее «приверженность дальнейшему эволюционному укреплению стабильности, безопасности и внутренней совместимости системы доменных имён (DNS) Интернета со всемирной перспективы и на благо глобального Интернет-сообщества, на основе равноправных взаимоотношений».

5.1.2.3 Кроме того, ICANN отвечает за работу корневого именного сервера под названием l.root-servers.net. В этой оперативной роли сотрудники ICANN также взаимодействуют на оперативном уровне с операторами прочих корневых серверов. Как оператор L-корня ICANN также принимает участие в деятельности сообщества DNS, включая вклад в такие инициативы сообщества, как «Система доменных имён – операционный, аналитический и исследовательский центр» (DNS-OAИЦ) и исследовательский проект «Один день из жизни Интернета» Кооперативной ассоциации по анализу данных Интернета (КААДИ). ICANN привержена к использованию своей деятельности для поддержки многообразия и понимания передового опыта, а также стремится приобретать и передавать знания.

## 5.2 Безопасность, стабильность и отказоустойчивость реестров и регистраторов ДВУ

Фундаментальной и непосредственной ответственностью ICANN, связанной с безопасностью, стабильностью и отказоустойчивостью Интернета, является управление соглашениями с реестрами рДВУ и аккредитованными ICANN регистраторами, и базовая структура соглашений, используемых для управления отношениями с реестрами рДВУ. ICANN заключила договора с 16 реестрами рДВУ и более чем 900 аккредитованными регистраторами, несущими ответственность за координацию доменных имён и обеспечение их нахождения в DNS. Обязанности сторон, с которыми заключены

договоры, очерчены в реестровых соглашениях (РА) и соглашениях об аккредитации регистраторов (САР). ICANN стремится защищать владельцев регистраций и способствовать поддержанию безопасности, стабильности и отказоустойчивости DNS и Интернета в целом посредством положений в упомянутых соглашениях. В последние десять лет ICANN стремилась укрепить эти соглашения путём включения положений, улучшающих стабильность и отказоустойчивость, как описано ниже.

### 5.2.1 Реестры рДВУ

5.2.1.1 ICANN сотрудничает с операторами рДВУ в свете безопасной и стабильной координации этих ДВУ. Кроме того, у каждого из реестров рДВУ заключён контракт с ICANN. При том, что некоторые элементы этих контрактов могут отличаться, положения, касающиеся безопасности, стабильности и отказоустойчивости остаются неизменными. В этих соглашениях содержится положение, требующее от операторов реестров реализовывать временные спецификации и политики, установленные ICANN и согласованные политики, разработанные организацией поддержки родовых имён (ОПРИ) и принятые ICANN. Прочие положения соглашений, способствующие безопасной и стабильной работе реестров, включают требования передачи информации на ответственное хранение третьим сторонам, а также соглашения об уровне услуг DNS, совместной регистрационной системе и операциях именного сервера. В контрактах между ICANN и рДВУ указывается готовность, уровни эксплуатационных показателей и требования к центрам обработки данных. В 2007 г. ICANN инициировала усилия по планированию непрерывности работы рДВУ, приведшие к формулированию рабочего плана, а также принятию обязательств по проведению ряда ежегодных учений по плану с целью повысить способность сообщества реестров рДВУ справляться с проблемами или недостатками системы реестров и регистраторов.

5.2.1.2 В 2006 году ICANN ввела процесс оценки услуг реестров (ПОУР; Registry Services Evaluation Process, RSEP) в качестве средства обеспечения оперативного и предсказуемого механизма ввода новых услуг реестров. Ключевым компонентом ПОУР является определение потенциала предложенной услуги представлять угрозу безопасности или стабильности. Если устанавливается, что предлагаемая услуга способна представлять угрозу безопасности или стабильности, предложение передаётся

на рассмотрение панели технических экспертов под названием группа технической оценки услуг реестра (ГТОУР). ГТОУР производит анализ предлагаемой услуги и представляет Правлению ICANN рекомендацию одобрить или отклонить услугу.

### 5.2.2 Новые рДВУ и ИДИ

5.2.2.1 Ведя подготовку к открытию механизмов регистрации новых ДВУ для включения ИДИ, ICANN признаёт необходимость предпринимать усилия по обеспечению безопасной, стабильной и отказоустойчивой работы новых участников DNS и всей системы в целом. Процесс подачи и анализа заявок на новые рДВУ включает техническую оценку способности заявителя заведовать реестром, а также соответствие строкой техническим предписаниям, выраженным в ЗоК, согласно протоколу об интернационализации доменных имён в приложениях (ИДИП) и руководстве по ИДИ. Ввод нДВУ с ИДИ будет осуществляться с использованием другого процесса, так как первоначально он будет ограничен строками, не вызывающим споров, представляющими названия стран и территорий, соответствующие существующим нДВУ. В июле 2007 г. ККБС представил комментарии по воздействию ИДИ на безопасность и стабильность DNS на корневом уровне, проинформировав представителей процессов планирования реализации и тестирования.

5.2.2.2 Техническая оценка заявителей и предлагаемых ими ДВУ будет производиться независимой группой экспертов. Кроме того, механизм внедрения новых рДВУ предполагает предварительную реализацию процесса ПОУР для оценки возможных вопросов безопасности и стабильности новых услуг реестров, предлагаемых в заявке на рДВУ. В случае ДВУ с ИДИ технические требования к строкам и соответствующий процесс оценки одинаковы для рДВУ с ИДИ и нДВУ с ИДИ.

Кроме того, от всех заявителей перед делегирование домена требуется прохождение технической проверки соответствия ими техническим требованиям для эксплуатации реестра.

### 5.2.3 Регистраторы рДВУ

5.2.3.1 По вопросам безопасности, стабильности и отказоустойчивости ICANN также сотрудничает с регистраторами. С договорной точки зрения взаимоотношения ICANN с регистраторами строятся на основе стандартного соглашения об аккредитации

регистратора (CAP). В CAP устанавливаются некоторые стандарты сбора, удержания и ответственного хранения данных. В CAP также включаются (по ссылке) согласованные политики, разработанные сообществом ICANN, такие как политика изменения регистраторов, политика напоминания о данных Whois и политика точности восстановленных имён, помимо прочих, которые различными способами содействуют безопасности, стабильности и отказоустойчивости.

5.2.3.2 Сотрудники отдела по связям с регистраторами ICANN выполняют роль первой линии связи при рутинном отслеживании соответствия регистраторами требованиям CAP путём неформального разрешения жалоб регистрирующихся и разногласий между регистраторами, а также путём периодического анализа аккредитации (например, после обновления CAP регистратора).

5.2.3.3 В поддержку более стабильной системы доменных имён ICANN разработала программы и механизмы на случай возможного разорения регистратора. Так например, ICANN реализовала программу ответственного хранения данных регистраторов, в рамках которой от регистраторов требуется ежедневно или еженедельно передавать резервные копии регистрационных данных на ответственное хранение. Процедура изменения регистратора, лишившегося аккредитации, облегчает оперативный перевод регистраций от регистратора, лишившегося регистрации, регистратору, аккредитованному ICANN. Кроме того, сотрудники ICANN используют ряд внутренних оперативных механизмов, направленных на способствование поддержанию здоровой среды регистрации доменов и предотвращение нарушений в работе регистраторов и пользователей Интернета в случае разорения регистратора.

### 5.2.4 Whois

5.2.4.1 Службы WHOIS (произносится «ху из») предоставляют общий доступ к информации по зарегистрированным доменным именам, которая в настоящий момент включает в себя контактные данные держателей зарегистрированных имен. ICANN играет определённую роль в администрировании разработанных сообществом правил для системы Whois в рамках рДВУ. Объём данных, собираемых при регистрации доменного имени, и способы, которыми можно получить доступ к этим данным, указываются в соглашениях, заключаемых ICANN по доменным именам, зарегистрированным в рДВУ.

Например, ICANN требует от аккредитованных регистраторов собирать названия зарегистрированных доменов, их именных серверов и регистраторов, даты создания создания доменов и сроки их истечения, контактную информацию зарегистрированного держателя имени, реквизиты для связи по техническим и административным вопросам и предоставлять к ним бесплатный открытый доступ.

5.2.4.2 Whois применяется различными сообществами для ряда целей, включая способствование технической координации содействие обеспечению информации об организациях и лицах, подозреваемых в возможных злоупотреблениях DNS. Деятельность ICANN сосредоточена на обеспечении выполнениями реестрами рДВУ и аккредитованными ICANN регистраторами их договорных обязательств. При рассмотрении изменений политики Whois сообщество ICANN допускает легитимное использование системы Whois для оказания содействия лицам и организациям, борющимся со злоупотреблениями DNS, стремясь при этом сбалансировать широкую палитру мнений сторон, заинтересованных в способе функционирования системы Whois. ICANN признаёт обоснованность озабоченности вопросами конфиденциальности и безопасности, выражаемой различными лицами по поводу предоставления их информации посредством Whois.

### 5.2.5 Выполнение договорных обязательств

5.2.5.1 Отдел выполнения договорных обязательств обеспечивает выполнение со стороны ICANN и её партнёров по договорам требований, установленных в соглашениях между сторонами. В его задачи входит управление системой ICANN по приёму жалоб, позволяющей общественности регистрировать жалобы, связанные с доменными именами, которые могут относиться к вопросам безопасности, стабильности или отказоустойчивости. Дополнительная информация доступна на веб-сайте http://reports.internic.net/cgi/registrars/problem-report.cgi. Сотрудники отдела выполнения обязательств проверяют жалобы, связанные с возможными нарушениями САР, а при выявлении нарушений договора принимаются меры по их устранению. Так как большая часть жалоб, получаемых посредством данной системы относится к вопросам, находящимся вне компетенции ICANN (например, спам, содержимое веб-сайтов, обслуживание

клиентов регистраторами) ICANN переадресует такие жалобы регистраторам.

5.2.5.2 Отдел выполнения договорных обязательств также управляет системой отчётов о проблемах данных Whois (СОПД-W), доступ к которой находится по адресу http://wdprs.internic.net/. СОПД-W создана для содействия регистраторам в выполнении их обязательств по проверке подозреваемых неточностей в данных Whois. Эта система, разработанная в 2002 г., позволяет общественности регистрировать заявления о неточностях в данных Whois, которые затем передаются регистраторам для принятия соответствующих мер. На основании консультаций с регистраторами и постоянными группами интеллектуальной собственности (ПГИС) в 2008 году в СОПД-W были внесены изменения, призванные решить ряд вопросов, поднятых Интернет-сообществом, включая ограниченную функциональность, ограниченную мощность и недостаток механизмов отслеживания дальнейшего соблюдения обязательств. Видоизменённая СОПД-W была запущена в декабре 2008 г. Отдел выполнения договорных обязательств продолжает дорабатывать эту систему с целью повышения точности данных Whois.

### 5.2.6 Защита владельцев регистраций рДВУ

5.2.6.1 ICANN также стремится различными способами обеспечивать уверенность владельцев регистраций в безопасности, стабильности и отказоустойчивости DNS. Защита в этих областях предоставляется посредством положений в контрактах, соглашениях и программах обеспечения выполнения договоров ICANN. ICANN предоставляет владельцам регистраций сведения об обязательствах регистраторов по CAP и способ регистрации жалоб через сайт InterNIC http://www.internic.net/. ICANN также ведёт разъяснительную деятельность в сообществе регистраторов, поощряя поддержку IPv6 для лиц, регистрирующих домены.

5.2.6.2 Помимо этого работа организаций поддержки и консультативных комитетов ICANN сосредоточена на решении вопросов, касающихся безопасности, стабильности и отказоустойчивости, возникающих у владельцев регистраций. В консультациях ККБС регистраторам рекомендуются практики по улучшению защиты доменных имён и противодействию использованию «fast flux», злоупотреблениям данными

Whois и неправомерному использованию имён, а также решению вопросов, возникающих у владельцев регистраций, в том числе и в отношении их обновления. Не только ККБС, но и расширенный консультативный комитет (АЛАК) поднимает вопросы, касающиеся защиты владельцев регистраций. АЛАК первым поднял вопрос о пробном использовании доменов, что привело к принятию Советом ОПРИ и Правлением новой согласованной политики, направленной на предотвращение злоупотреблений периодом пробного использования доменов. Не так давно АЛАК консультировал Совет ОПРИ по вопросу восстановления владельцами регистраций доменных имён после истечения срока их действия. ОПРИ также предпринимает ряд дополнительных инициатив, обладающих потенциалом привести к улучшению защиты владельцев регистраций, таких как улучшения политики изменения регистраторов, включая соображения по необходимости электронной аутентификации и доработки политики в сфере политик относительно хостинга «fast flux» и злоупотреблений при регистрации.

### 5.2.7 нДВУ

Взаимодействие ICANN с реестрами нДВУ направляется общим пониманием того, что реестры нДВУ и ICANN должны поддерживать и повышать безопасность, стабильность и отказоустойчивость DNS на пользу местным и глобальным пользователям Интернета. Это отражено в структурной программе подотчётности, составляющей основу ряда соглашений между отдельными реестрами нДВУ и ICANN. Основное внимание ICANN при совместной с нДВУ работе по укреплению безопасности, стабильности и отказоустойчивости уделяется сотрудничеству с третьими сторонами по предоставлению платформы для обмена информацией и взаимодействия, технического обучения, направленного на улучшение понимания ключевых вопросов, и развитие мощностей для планирования реагирования на нападения и чрезвычайные происшествия. Персонал ICANN тесно сотрудничает с операторами ДВУ, информируя последних по вопросам безопасности через функции IANA, программу планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП) и усилия региональных представителей отдела глобальных партнёрств. Через функции IANA ICANN развила доверительные отношения с операторами ДВУ благодаря улучшению своих рабочих показателей и разъяснительной работы в сообществе операторов ДВУ, что способствует осуществлению совместного реагирования в требующих глобальной координации ситуациях, связанных с DNS.

### 5.2.8 Технические требования IANA

Посредством управления функций IANA ICANN также помогает обеспечить соответствие ДВУ техническим стандартам в поддержку стабильной и безопасной работы. Конкретные требования к именным серверам обеспечивают готовность доменов в DNS, а персонал, ответственный за функции IANA, тесно сотрудничает с менеджерами ДВУ по решению проблем, возникающих у последних при соблюдении этих технических стандартов. ICANN не вмешивается в эксплуатацию нДВУ, но готова оказывать содействие в ситуациях, где необходимо быстро и надёжно вносить изменения в их корневые данные. Основная цель ICANN – обеспечить стабильность и безопасность зоны ДВУ и корневой зоны.

### 5.2.9 Совместное реагирование на злоупотребления системой доменных имён

ICANN сотрудничает с рядом организаций, стремясь обеспечить субъектам возможность анализировать деятельность, которая может представлять собой злоупотребление DNS. С конца 2008 г. значительно активизировалось распространение зловредных программ, использующих ресурсы DNS. ICANN активно сотрудничает с реестрами и регистраторами, обеспечивая наличие понимания проблематики и способствуя распространению информации. Мандат ICANN в этой области ограничен, и поэтому корпорация как одна из организаций такого рода принимает участие в обсуждениях обеспечения эффективного реагирования на возникновение конкретных рабочих ситуаций.

### 5.2.10 Обеспечение общей безопасности и отказоустойчивости DNS

5.2.10.1 Хотя ни одна организация не несёт общей ответственности по данному вопросу, сотрудники ICANN, организаций поддержки и консультативных комитетов способствуют повышению общей стабильности, безопасности и отказоустойчивости DNS. С момента своего основания ККБС обеспечивает анализ и рекомендации для сообщества DNS. Среди ключевых усилий можно привести анализ и рекомендации, связанные с нападениями на в виде распределённого отказа в обслуживании (Distributed Denial-of-Service, DDoS), внедрение DNSSEC с добавлением IPv6 записей в корень DNS, упреждённое использование доменных имён, хостинг «fast flux» и захват доменных имён. Кроме того, члены ККБС принимают участие в комитете

Интернет-политики рабочей группы по борьбе с фишингом (РГБФ) и выступают соавторами проектов документов, в которых описываются способы злоупотребления доменными и суб-доменными именами со стороны фишеров.

5.2.10.2 ICANN планирует и в дальнейшем развивать эту роль стремясь определять возможности для сотрудничества по всему сообществу, а также определять и снижать риски, которым подвержены системы. ICANN инициировала усилия по улучшению понимания и сокращению общесистемных рисков для DNS в ходе своего глобального симпозиума по безопасности, стабильности и отказоустойчивости DNS, прошедшего в феврале 2009 г. и организованного в сотрудничестве с Техническим центром безопасности информации штата Джорджия (GTISC). Основное внимание на симпозиуме уделялось пониманию рисков, связанных с DNS, на крупных предприятиях, сложностях обеспечения безопасных, стабильных и отказоустойчивых операций DNS в развивающихся странах и борьбе со злоупотреблениями DNS в противозаконных целях. С отчётом можно ознакомиться по адресу http://www.gtisc.gatech.edu/icann09.

5.2.10.3 Кроме того, сотрудники ICANN, организации поддержки и консультативные комитеты ICANN начали повышать интенсивность сотрудничества с рядом полисубъектных проектов с целью повысить способность корпорации осуществлять эффективное формулирование политики, обеспечивать выполнение договорных условий и по ряду других инициатив, связанных с решением задач в области безопасности и отказоустойчивости, стоящих перед DNS и вызываемых ей.

## 5.3 Сотрудничество с Организацией номерных ресурсов (ОНР) и региональными Интернет-реестрами (РИР)

Взаимодействие ICANN с Организацией номерных ресурсов (ОНР; Numbering Resource Organization, NRO) и региональными Интернет-реестрами (РИР) направляется общим пониманием необходимости поддержания и повышения безопасности, стабильности и отказоустойчивости Интернета со стороны РИР и ICANN на благо местных и глобальных пользователей Интернета ICANN принимает участие в ряде совместных проектов с этими

организациями, связанных с безопасностью, стабильностью и отказоустойчивостью Интернета. В частности, ICANN работала с этими организациями над установкой подписей DNSSEC на обратных участках дерева DNS. Являясь реестрами IP-адресов, РИР непосредственно вовлечены в усилия по обеспечению аутентификации адресов и маршрутов Протокола пограничного шлюза в рамках проекта КОИр, а ICANN будет продолжать стремиться сотрудничать с ними в рамках таких проектов.

## 5.4 Корпоративная безопасность ICANN и операции по непрерывности

5.4.1 ICANN обеспечивает безопасность, стабильность и отказоустойчивость собственных операций при руководстве IANA и прочих ключевых функциях, которые она осуществляет, как часть системы DNS и адресной системы, а также стремиться выполнять свои обязанности в качестве корпорации и общественного участника в обеспечении общей безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета.

5.4.2 ICANN работает над полномасштабной программой безопасности, управляющей риском в сферах информации, кадров и материальных активов. Осенью 2008 г. ICANN назначила директора по безопасности, несущего ответственность за эту программу. ICANN предоставляет информацию, обрабатывает чувствительные данные и полагается на использование информационных технологий (ИТ) при осуществлении своей деятельности. На основании плана информационной безопасности ICANN, соответствующего стандартам, установленным в ISO 27002, ведутся улучшения процедур и механизмов поддержки. План информационной безопасности ICANN также включает предоставление министерству торговли США плана информационной безопасности IANA и управление проведением сторонних проверок его программы. Планирование безопасности персонала сосредоточено на защите сотрудников ICANN на обоих основных местах работы и при осуществлении ими глобальной деятельности ICANN, включая обеспечение безопасности на конференциях ICANN. ICANN установила процесс планирования по управлению рисками, связанными с безопасностью персонала и использует собственный отдел безопасности наряду с поддержкой консультантов

по безопасности. ICANN установила процесс планирования для управления рисками, связанными с физическими объектами, включая основное здание корпорации в Марина-дель-Рей, Калифорния, США, а также узловые офисы и резервные объекты.

5.4.3 Программы безопасности ICANN являются частью общей программы управления корпоративными рисками, реализуемой под наблюдение Правления ICANN, а также взаимно поддерживающих друг друга корпоративных программ непрерывности деятельности. По мере роста ICANN растёт и база активов корпорации наряду с масштабами её международной деятельности и общественной значимостью. Среда корпоративной безопасности ICANN всё более усложняется, и корпорация продолжит уделять особое внимание управлению рисками, непрерывности и безопасности деятельности как фундаментальным составляющим своего корпоративного механизма.

## 5.5 Деятельность организаций поддержки и консультативных комитетов ICANN

5.5.1 Широкое сообщество ICANN также играет важнейшую роль в обеспечении безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов в ходе процесса формулирования политики на основе инициатив, исходящих от простых участников. ICANN располагает тремя организациями поддержки – Организацией поддержки родовых имён (ОПРИ), Организацией поддержки национальных имён (ОПНИ) и Организацией поддержки адресов (ОПА), несущими ответственность за разработку политик с учётом вопросов, связанных с безопасностью и стабильностью. Подробности, касающиеся каждой организации поддержки и её механизмов, можно найти по адресам: http://gnso.icann.org, http://ccnso.icann.org/ и http://aso.icann.org/. Эти организации предоставляют рекомендации, которые должны быть одобрены Правлением ICANN с тем, чтобы быть реализованными посредством ряда контрактов, соглашений, меморандумов о понимании и действий сотрудников. ОПРИ прежде всего отвечает за политики, связанные с соглашениями реестров и регистраторов рДВУ с учётом изменения политики Whois рДВУ, анализ вопросов, связанных, среди прочего, с хостингом «fast flux»,

истечением срока действия доменных имён, изменением регистраторов доменных имён и политиками по борьбе со злоупотреблениями при регистрации.

5.5.2 В данный момент ICANN работает с сообществом над пересмотром существующего процесса разработки политики (ПРП) рДВУ для повышения его эффективности и чуткости к нуждам корпорации в сфере разработки политики. Среди многочисленных изменений, предусмотренных в существующем ПДП, имеются и изменения, направленные на привлечение дополнительного технического опыта, работы по исследованиям и установлению фактов на ранних этапах процесса, с целью способствовать более информированному и осознанному определению и направлению сложных задач в сфере формулирования политики, а также на разработку улучшенных способов оценки эффективности новых политик.

5.5.3 ОПНИ способствует сотрудничеству ICANN с нДВУ, включая обмен информацией, связанной с безопасностью, стабильностью и отказоустойчивостью.

5.5.4 ОПА разрабатывает политику, связанную с распределением блоков адресов IPv4 и IPv6 и блоков номеров АС РИР.

5.5.5 Кроме того, в ICANN существует четыре консультативных комитета, предоставляющие консультации Правлению и сообществу ICANN – расширенный консультативный комитет (АЛАК), правительственный консультативный комитет (ПКК), Консультативный комитет системы корневого сервера (ККСКС) и консультативный комитет по безопасности и стабильности (ККБС). Подробности, связанные с функциями, механизмами и деятельностью этих комитетов можно найти по адресу http://www.icann.org/en/committees/gac/. Эти консультативные комитеты часто сотрудничают между собой и с организациями поддержки по различным проектам, что, в первую очередь касается ККБС. Сотрудники отдела политик ICANN оказывают комитетам поддержку при проведении исследований, анализе и подготовке рекомендаций.

5.5.6 ККБС консультирует сообщество и Правление ICANN по вопросам, связанным с безопасностью и стабильностью систем распределения имён и адресов Интернета. К таким вопросам относятся правильное и надёжное функционирование корневой системы имён,

распределение адресов и назначение Интернет-номеров, а также услуги реестров и регистраторов рДВУ, такие как Whois. ККБС занимается постоянной оценкой угроз и анализом рисков для служб распределения имён и адресов Интернета с целью определения источников основных угроз стабильности и безопасности, и предоставляет соответствующие рекомендации сообществу ICANN. Подробности о деятельности ККБС можно найти по адресу www.icann.org/en/committees/security.

5.5.7 Помимо упомянутого выше, организации поддержки и консультативные комитеты занимаются совместными обсуждениями на конференциях ICANN, где эти две группы обсуждают вопросы, связанные с безопасностью стабильностью, представляющие для них обоюдный интерес, организацией семинаров и брифингов по вопросам, связанным с безопасностью и стабильностью, а также оповещением сообщества о деятельности, связанной с политикой, посредством ежемесячного отчёта о политике (http://www.icann.org/en/topics/policy/).

## 5.6 Глобальная деятельность по повышению безопасности, стабильности и отказоустойчивости

### 5.6.1 Глобальные партнёры и проекты

Суть стратегии глобальной деятельности ICANN в отношении безопасности, стабильности и отказоустойчивости заключается в том, чтобы развивать и использовать существующие результаты работы, осуществляемой отделом глобальных партнёрств. ICANN принимает активное участие в широком ряде международных форумов, связанных с Интернетом, включая несколько, посвящённых вопросам безопасности, стабильности и отказоустойчивости Интернета. Перечень партнёров и проектов, приведённый ниже, не является исчерпывающим, и ICANN будет стремиться принимать участие и в других по мере возникновения возможностей. Корпорация имеет следующих ключевых глобальных партнёров.

- Комиссия по технологиям Интернета (IETF) / Совет по архитектуре Интернета (IAB): возглавляют усилия по определению технологических подходов к повышению безопасности Интернета, сосредоточенные на разработке более мощных протоколов и рабочих практик. ICANN

сотрудничает с IETF над созданием протоколов, связанных с назначением имён и адресов, и стремится обеспечивать их внедрение в ядре Интернета, способствуя обеспечения безопасности общей среды. В частности, ICANN принимает участие в усилиях по созданию протоколов, обеспечивающих более безопасное основание для Интернета, и сосредоточенных на таких проектах как DNSSEC и КОИр.

- Общество Интернета (ISOC): Стимулирует осведомлённость о вопросах кибербезопасности и необходимости добиваться доверия к Интернету среди широких масс пользователей, в особенности, в развивающихся странах; в сотрудничестве с другими предоставляет техническое обучение, нацеленное на повышение безопасности и отказоустойчивости Интернета. ICANN сотрудничает с ISOC над обеспечением осведомлённости и расширением возможностей для поддержания безопасности, стабильности и отказоустойчивости. ICANN планирует продолжать сотрудничество в рамках продолжающейся совместной программы ISOC и ICANN по обеспечению образовательных курсов для операторов ДВУ, включающих техническое обучение тому, как повышать безопасность, сокращать последствия кибер-атак и сбоев.
- Форум управления Интернетом (IGF): IGF поддерживает диалоги по кибербезопасности и доверию между различными субъектами. Кроме того, IGF выработал подход к управлению ключевыми ресурсами Интернета и борьбе с киберпреступлениями. ICANN продолжит участвовать в IGF, включая распространение информации о своей собственной роли в обеспечении безопасности, стабильности и отказоустойчивости систему уникальных идентификаторов Интернета, а также вносить свою лепту в глобальный диалог, ведущийся на данном форуме.
- Операционный, аналитический и исследовательский центр DNS (DNS-ОАИЦ): ICANN продолжит оставаться спонсором и активным участником всего спектра проектов DNS-ОАИЦ.

### 5.6.2 Региональные партнёры и проекты

ICANN устанавливает региональные связи с разнообразными партнёрами и в рамках разнообразных проектов. Ключевые аспекты региональной деятельности ICANN представлены ниже.

- ***Региональные ассоциации нДВУ*** – помимо сотрудничества по программе ПРНЧП, описанного ниже, ICANN продолжит предоставлять содействие и специальные знания в рамках проектов, спонсируемых этими организациями.

- ***Региональные сетевые инфоцентры (РСИ) и группы сетевых операторов (ГСО)*** – ICANN продолжит участвовать в этих форумах в обеспечение того, что деятельность корпорации наилучшим образом позволяет осуществлять безопасные и отказоустойчивые сетевые операции, включая координацию функций IANA.
- ***Азия*** – в мае 2008 г., в Куала-Лумпур ICANN инициировала программу обучения в области безопасности и отказоустойчивости нДВУ в сотрудничестве с Азиатско-Тихоокеанской ассоциацией ДВУ (APTLD), которая с тех пор продолжает пользоваться мощной поддержкой для осуществления деятельности в указанном регионе. ICANN продолжит принимать участие в региональных форумах, таких как основы управления Интернет-ресурсами, с целью предоставления операционных консультаций и обучения, связанных с безопасностью и отказоустойчивостью DNS по мере возникновения возможностей.
- ***Европа*** – ICANN продолжит участвовать в усилиях Европейского агентства по сетевой и информационной безопасности (ENISA), связанных с DNSSEC и повышением отказоустойчивости DNS в рамках более широких усилий Европейской комиссии, направленных на защиту ключевых элементов инфраструктуры. ICANN будет сотрудничать с Советом европейских национальных реестров доменов верхнего уровня (CENTR) по проведению учебных семинаров по безопасности и отказоустойчивости нДВУ, инициированных в связи с 58-ым заседанием RIPE в мае 2009 г. в Амстердаме. ICANN продолжит сотрудничество с Институтом проблем информационной безопасности (ИПИБ) Московского государственного университета по расширению международного диалога по кибербезопасности. В частности, в 2008 и 2009 гг.. ICANN и ИПИБ провели совместные семинары в г. Гармиш, Германия при поддержке Германско-американского маршалловского центра стратегических исследований, и обе организации планируют продолжать сотрудничество.
- ***Африка и Латинская Америка*** – совместно с региональными организациями ISOC, а также в рамках прочих соответствующих форумов ICANN продолжит осуществлять проекты, связанные с кибербезопасностью. В преддверии 34-й международной открытой конференции ICANN, прошедшей в марте 2009 г., совместно с ассоциацией LACTLD корпорация предлагала курсы подготовки в области безопасности и отказоустойчивости нДВУ, а теперь планирует и дальнейшие совместные мероприятия. ICANN также проводит курсы в области нДВУ совместно с ассоциацией африканских доменов верхнего уровня (AfTLD) и ISOC-Africa. Эти проекты были

инициированы в апреле 2009 г. на конференции Организации африканских доменов верхнего уровня (AFTLD) в г. Аруша, Танзания.

### 5.6.3 Работа с правительствами

ICANN сотрудничает с правительствами по всему миру в стремлении обеспечить безопасность, стабильность и отказоустойчивость систем уникальных идентификаторов Интернета. ICANN продолжит предоставлять свой технический и операционный взгляд на способы улучшения безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета. ICANN понимает, что к этим системам следует относиться как к ключевым элементам инфраструктуры. В рамках ICANN Правительственный консультативный комитет (ПКК) будет получать регулярные отчёты об усилиях корпорации в области безопасности, стабильности и отказоустойчивости и вносить свой вклад в эти программы в рамках процесса стратегического планирования. На уровне межправительственных организаций ICANN продолжит активно определять свою роль в международных обсуждениях вопросов безопасности и их значении для способов управления безопасностью и отказоустойчивостью систем уникальных идентификаторов. Можно перечислить следующие ключевые аспекты работы.

- ***Международный союз электросвязи (МСЭ)*** – МСЭ претворяет в жизнь Глобальный план кибербезопасности (ГПК), определяемый как «структура для международного сотрудничества, нацеленного на повышение доверия и безопасности информационного общества». В рамках этого широкого проекта сектор развития телекоммуникаций МСЭ, называемый МСЭ-Р, подготовил широко направленную программу по работе с развивающимися странами для повышения осведомлённости на национальном уровне и содействия программам развития мощностей, связанным с повышением кибербезопасности. ICANN продолжит анализировать перспективы партнёрских отношений с МСЭ в отношении усилий союза по кибербезопасности, направленным на разъяснительную деятельность, повышение осведомлённости и расширение мощностей, с упором на техническую роль корпорации в обеспечении безопасности и отказоустойчивости DNS.
- ***Организация экономического сотрудничества и развития (ОЭСР)*** – ICANN продолжит участвовать в форумах по кибербезопасности, как например, в продолжающихся усилиях ОЭСР по борьбе со зловредными программами.

ICANN также продолжит участвовать в родственных проектах АТЭС в этой области.

- ***Прочие международные организации и региональные экономические комиссии ООН*** – ICANN будет сотрудничать с другими международными организациями и экономическими комиссиями ООН, направляя свои усилия на содействие региональным проектам, нацеленным на повышение безопасности и отказоустойчивости DNS. Такие проекты будут основываться на меморандумах о взаимопонимании, заключённых ICANN с рядом организаций.

# 6. Планы ICANN по повышению безопасности, стабильности и отказоустойчивости на FY10

Проекты ICANN, связанные с укреплением безопасности, стабильности и отказоустойчивости, и ресурсы, выделяемые на них, определяются механизмами стратегического и операционного планирования. В проекции на 2009-2010-ый операционный год ICANN планирует призвать к проведению ряда следующих ключевых инициатив.

- ***Операции IANA*** – оказывать поддержку, образовывать и вести подготовку к внедрению DNSSEC на корневом уровне, как записано в стратегическом плане ICANN на 2009-2012 гг., а также улучшать управление корневой зоной посредством автоматизации и методы аутентификации сообщений, обмениваемых с менеджерами ДВУ.
- ***Операции корневого сервера DNS –*** продолжение стремления к взаимному признанию ролей и ответственностей и инициирование добровольных усилий, направленных на осуществление планирования и проведение учений на случай чрезвычайных происшествий.
- ***Реестры рДВУ –*** обеспечить дальнейшую безопасность деятельности в ходе оценки оценки заявок от новых рДВУ и ИДИ . ICANN продолжит дорабатывать план бесперебойной работы реестров рДВУ и тестировать систему ответственного хранения данных.
- ***Реестры нДВУ –*** ICANN расширит сотрудничество в области доработки совместной программы планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП), введённой в сотрудничестве с ОПНИ и региональными ассоциациями ДВУ.
- ***Выполнение договорных обязательств –*** ICANN продолжит расширять масштабы деятельности по обеспечению выполнения договорных обязательств, связанных с рДВУ, и начнёт проведение аудиторских проверок субподрядчиков в рамках исполнения поправок к соглашению об аккредитации регистраторов от 9 марта и определение потенциальной вовлечённости субподрядчиков в злоумышленную деятельность для принятия исправительных мер.
- ***Реагирование на предумышленное злоупотребление системой доменных имён –*** ICANN продолжит развивать сотрудничество усилия, направленные против злоумышленного поведения, связанного с использованием

DNS, и способствовать обмену информацией для обеспечения эффективного реагирования.

- ***Внутренние операции ICANN по обеспечению безопасности и непрерывности*** – ICANN продолжит реализацию программ безопасности в рамках общих программ управления корпоративным риском, управления кризисными ситуациями и программ непрерывности деятельности. Основное внимание будет уделено устройству крепкого фундамента задокументированных планов и вспомогательных процедур.
- ***Обеспечение повсеместного участия и сотрудничества*** – ICANN будет расширять партнёрские отношения с такими организациями, как Комиссия по технологиям Интернета (Internet Engineering Task Force, IETF), Общество Интернета (Internet Society, ISOC), региональные Интернет-реестры и группы операторов сетей, операционного, аналитического и исследовательского центра DNS (DNS-ОАИЦ; Operations, Analysis and Research Center, DNS-OARC). ICANN также будет принимать участие в межнациональных диалогах, направленных на расширение понимания трудностей с сфере безопасности, стабильности и отказоустойчивости, стоящих перед экосистемой Интернета, и способов решения этих трудностей при участии большого количества субъектов.

Полный перечень проектов разъясняется ниже. В приложении A указаны конкретные цели, участники, результаты и ресурсные требования, запланированные на FY10.

## 6.1 Ключевые функции DNS и адресной системы

### 6.1.1 Операции IANA

ICANN продолжит руководство функциями IANA и работу по улучшению эксплуатационных показателей её проектов в сотрудничестве с министерством торговли США, фирмой VeriSign, РИР и операторами ДВУ.

6.1.1.1 Сотрудничество с партнёрами по управлению корневой зоной, министерством торговли США и VeriSign, по реализации механизма DNSSEC-подписания корневой зоны. ICANN продолжит добиваться внедрения процесса, описанного в предложении от сентября 2008 г. Согласно приоритетам, изложенным в стратегическом плане на 2009-2012 гг. ICANN достигнет операционной готовности для внедрения DNSSEC в корневой зоне к концу 2009 г. ICANN предложила подход, обеспечивающий продолжение бесперебойной работы механизма

распределения корневой зоны DNS: ввод совместной ответственности ICANN, VeriSign, NTIA и операторов корневых серверов за работу DNSSEC. ICANN предложила гибкие решения, включающие промежуточный подход, способный перерасти в постоянное решение, и уже провела операционную подготовку для выполнения своей роли.

ICANN также будет осуществлять ряд проектов, позволяющих расширить DNSSEC по всей DNS. ICANN обеспечит включение в свою программу механизмов изменения регистраторов и создания необходимых для этого счетов ответственного хранения, а также продолжит обсуждения с заитересованными сторонами по конкретным вопросам внедрения. ICANN будет продолжать поддержку репозитория IANA для отметок о доверии для доменов верхнего уровня (РОД-I) до тех пор, пока корневая зона не будет подписана. ICANN продолжит добиваться разрешения на подписание зон .int и .arpa. ICANN поддержит внедрение DNSSEC путём подписания зон, управляемых корпорацией, включая icann.org и iana.org, управления исптытательной площадкой распространения полученного опыта среди субъектов, вовлечённых во внедрение DNSSEC.

6.1.1.2 Среди конкретных инициатив по улучшению функций IANA можно перечислить следующие.

- Улучшение управления корневой зоной посредством автоматизации (ПО eIANA/RZM); улучшенная аутентификация сообщений с менеджерами ДВУ; пересмотр механизмов и практик из соображение безопасности и оптимизации
- Поддержка разработки и внедрения безопасного выделения и назначения IP-адресов через КОИр или другие механизмы, принятые РИР и сообществом Интернет-маршрутирования при продолжающейся поддержке рабочей группы IETF защищённого репозитория разведывательных данных (ЗРРД).
- Сотрудничество с техническими и операционными сообществами по определению, анализу и возможному внедрению дополнительных технических требований или стандартов для повышения безопасности, стабильности или отказоустойчивости DNS.

### 6.1.2 Операции корневого сервера DNS

6.1.2.1 ICANN продолжит стремиться к взаимному признанию ролей и ответственности с операторами корневой зоны в рамках своей общей роли по координации DNS. ICANN

также стремится способствовать реализации более надёжных механизмов координации в рамках сообщества операторов корневой зоны в отношении мер, способствующих безопасности, стабильности и отказоустойчивости. В своём качестве L-оператора ICANN планирует сотрудничать с прочими операторами корневой зоны по инициации добровольных усилий по осуществлению планирования и упражнений, направленных на повышение отказоустойчивости систем корневого сервера на случай ряда стрессовых чрезвычайных обстоятельств.

6.1.2.3 ICANN планирует продолжать улучшать деятельность L-корня. Кроме того, ICANN привлекла DNS-ОАИЦ к исследованию влияния изменений, включая ввод новых рДВУ и ИДИ, внедрение IPv6 и возможное внедрение DNSSEC-подписей корневой зоны, на функционирование отдельной секции корневого сервера на основе модели L-корня. В более широком смысле ККСКС и ККБС проводят совместное исследование безопасности и стабильности корневого сервера в свете предполагаемых изменений, описанных в разделе 6.6.

## 6.2 Взаимоотношения с реестрами и регистраторами ДВУ

### 6.2.1 Реестры рДВУ

ICANN продолжит продолжит контрактную координацию, связанную с операциями рДВУ, включая приложения для проверки новых услуг через ПОУР. ICANN требуется, чтобы в анализ включались предложения, требующие активирования ГТОУР для оценки вопросов безопасности, стабильности и отказоустойчивости. ICANN продолжит прилагать усилия по поощрению сотрудничества с сообществом и использованию передового опыта в сфере безопасности, стабильности и отказоустойчивости путём проведения региональных семинаров ICANN для реестров и регистраторов, участия в ряде форумов сообщества и распространения информации через свой собственный веб-сайт. Кроме того, ICANN планирует сотрудничать с DNS-ОАИЦ по созданию портала для обмена информацией о передовом опыте и совместных усилий в области безопасности, стабильности и отказоустойчивости, предназначенного для использования всем сообществом реестров.

### 6.2.2 Новые рДВУ

На протяжении всего грядущего года основное внимание в сфере безопасности, стабильности и отказоустойчивости будет привлечено к потенциальному внедрению механизмов, связанных с созданием новых рДВУ. В феврале 2009 г. Правление ICANN поручило ККСКС и ККБС провести совместное исследование потенциального воздействия на безопасность, стабильность и отказоустойчивость системы корневого сервера в целом ряда возможных изменений в DNS, включая внедрение новых рДВУ и ИДИ, а также возможное внедрение DNSSEC-подписей корневой зоны в течение ближайших 18 месяцев. Их отчёт о проведённом исследовании ожидается в сентябре 2009 г. ICANN также определит положения по оценке заявителей, чтобы убедиться, что они способны реализовывать технически безопасные операции, соответствующие положениям Whois, способны обеспечивать приемлемое планирование на случай чрезвычайных происшествий и обеспечивать защиту владельцев регистраций. ICANN продолжит дорабатывать план обеспечения непрерывности реестров нДВУ и программу учений, в которую войдёт тест системы передачи данных на ответственное хранение в режиме реального времени. ICANN также обеспечит создание и безопасную эксплуатацию автоматизированной системы для заявителей на ДВУ.

### 6.2.3 ИДИ

В том же ключе, усилия ICANN по обеспечению внедрения ДВУ с ИДИ (нДВУ и рДВУ) будут направлены на то, чтобы эти доменные имена, представленные местными символами, были безопасными, стабильными и отказоустойчивыми. ICANN продолжит сотрудничать с IETF в сфере создания Интернет-протоколов с целью завершения анализа и последующего одобрения безопасного и стабильного протокола ИДИ. В случае, если разработанный IETF протокол не будет полностью одобрен, то на основе рекомендаций технического сообщества ICANN может установить конкретные дополнительные требования к ДВУ с ИДИ, чтобы обеспечить их долгосрочную применимость и после завершения пересмотра протокола. ICANN продолжит способствовать усилиям реестров по сотрудничеству с поставщиками в обеспечение создания таблиц ИДИ, в как можно большей степени ограничивающие конфликты строк и путаницу и сокращают возможности для злоупотребления системой для недобросовестных целей. Для лиц, заинтересованных в том, чтобы стать оператором ДВУ с ИДИ, и нуждающихся в содействии и навыках в этой сфере, будет предоставлена функция поддержки с компетентностью в области ИДИ.

### 6.2.4 нДВУ

ICANN продолжит свои усилия, связанные с повышением безопасности, стабильности и отказоустойчивости нДВУ, путём сотрудничества с их нДВУ. В ближайшем году эта деятельность сосредоточится на доработке совместной программы планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП), введённой в сотрудничестве с ОПНИ и региональными ассоциациями ДВУ. Программа ПРНЧП сосредоточена на повышении безопасности и отказоустойчивости посредством профилактического планирования и повышенной способности к реагированию на полный спектр деструктивных угроз и рисков. В грядущем году программы будут расширяться и начнут включать техническое обучение, направленное на укрепление безопасности и отказоустойчивости в ответ на растущие угрозы и на предоставление помощи в разработке программ упражнений и оценки для планирования систем безопасности и реагирования на чрезвычайные происшествия. За следующий год ICANN планирует развить способность реализовывать программу ПРНЧП не только на английском языке и сотрудничать с Институтом программных технологий при Университете Карнеги-Меллона по применению его технологической структуры отказоустойчивости (TCO) в рамках добровольной программы по оценке уровня развития проектов в области безопасности, стабильности и отказоустойчивости ДВУ.

### 6.2.5 Регистраторы

ICANN продолжит разработку политики по повышению требований к регистраторам для получения аккредитации и в отношении передачи данных на ответственное хранение путём внесения улучшений в CAP. Помимо поддержки этих усилий сотрудники ICANN продолжат разрабатывать процедуры и механизмы в рамках существующих контрактов и политик по защите владельцев регистраций, а, в итоге, и по укреплению безопасности, стабильности и отказоустойчивости DNS. В частности, ведётся работа по усовершенствованию процедур оформления заявок на аккредитацию, повышению требований к желающим заключить CAP и ужесточению правил по отсеиванию, а также по разработке процедур, позволяющих регистраторам уходить с рынка ответственным образом. Ранее проделанная работа по развитию ответственного хранения данных и процедур расторжения договоров с регистраторами также послужит для укрепления текущих и будущих усилий ICANN по обеспечению выполнения договорных обязательств, позволяя отмену аккредитации регистраторов в случаях, когда их действия угрожают безопасности и стабильности DNS. ICANN продолжит формирование крепкого сообщества регистраторов посредством

разъяснительных мероприятий, позволяющих обмен передовым опытом в отрасли, и начнёт реализовывать новые каналы связи, предназначенные помочь регистраторам своевременно сообщать и реагировать на критические угрозы безопасности.

### 6.2.6 Выполнение договорных обязательств

6.2.6.1 ICANN продолжит расширять масштаб мер по обеспечению выполнения договорных обязательств, включая увеличение количества сотрудников соответствующего отдела. Среди важных новых сфер деятельности следует отметить инициирование проверок партнёров по договорам в рамках реализации поправок к соглашению об аккредитации регистраторов (CAP) от марта 2009 г. Кроме того, в 2009 году сотрудники отдела выполнения договорных обязательств будут работать совместно с сотрудниками отдела безопасности ICANN над выявлением партнёров по договорам, подозреваемых в злоумышленной деятельности. В случаях, когда доказывается осуществление злоумышленной деятельности партнёрами по договорам, могут быть приняты меры по обеспечению выполнения договорных обязательств. В прочих случаях для адекватного решения вопросов такого рода будут оповещаться правоохранительные и прочие соответствующие органы.

6.2.6.2 Отдел выполнения договорных обязательств в настоящий момент осуществляет исследования по оценке точности реквизитов для связи, содержащихся в данных Whois в системе рДВУ и степени, в которой владельцы регистраций используют службы конфиденциальности и прокси для сокрытия своей личности. Стремясь стимулировать выполнение договорных обязательств и доверие общественности, отдел выполнения договорных обязательств разрабатывает систему открытой публикации данных о лицах, в полной мере выполняющих свой обязательства. Система находится на ранней стадии разработки, а перед её внедрением будут проведены консультации с сообществами регистратором и реестров.

### 6.2.7 Совместное реагирование на злоупотребления системой доменных имён

Сотрудники ICANN также продолжать развивать совместные проекты, возникшие в ответ на недавние события, связанные с системой доменных имён, произошедшие с конца 2008 года, как например, меры принятые в связи с бот-сетью «Szirbi» и вирусом-

червём «Conficker» в конце 2008-го – начале 2009-го года. ICANN считает, что в подобном сотрудничестве должны участвовать реестры и регистраторы DNS, сообщество исследований в области безопасности и поставщики ПО и антивирусных программ. В частности, ICANN планирует сотрудничать с сообществами реестров и регистраторов по развитию сотрудничества в сфере борьбы со зловредным ПО, вирусами-червями и бот-сетями, использующими DNS для распространения и контроля. ICANN будет стремиться очертить процедуры связи и подтверждения действий реестров и регистраторов, а также способ своего участия, в случае такой необходимости, в обмене информацией с исследователями в области безопасности, поставщиками технологий и правоохранительными органами. ICANN обеспечить возможность для открытого обсуждения своих механизмов реализации совместного реагирования. Эти механизмы будут направлены на утверждение Правлению. Такое сочетание подходов обеспечит способность ICANN реагировать на запросы любых субъектов, которым может потребоваться её участие и сотрудничество.

### 6.2.8 Обеспечение общей безопасности DNS

Сотрудники ICANN будут стремиться развивать результаты симпозиума по безопасности, стабильности и отказоустойчивости DNS, прошедшего в феврале 2009 г., путём содействия ключевым совместным усилиям, связанным с сокращением операционных рисков для операторов и пользователей DNS. В планы входит созыв ежегодного симпозиума по пересмотру рисков, общих для вех DNS и преумножению возможностей для сотрудничества, не теряя из виду решение задач по обеспечению безопасности и стабильности DNS в развивающемся мире. ICANN также планирует сотрудничать с DNS-OAИЦ и форумом для бригад быстрого реагирования и безопасности, ФББР, уделяя основное внимание подготовке эффективных ответов на значительные ЧП и мероприятия в сообществе DNS. Кроме того, сотрудники ICANN продолжат отслеживать эволюцию планов по установлению системы назначения имён объектам и того, как такие планы могут включать DNS для обеспечения раннего определения некоторых потенциальных вопросов, связанных с безопасностью, стабильностью и отказоустойчивостью.

## 6.3 Взаимодействие с ОНР и РИР

ICANN планирует продолжать сотрудничество с ОНР и РИР и принимать участие в представляющей взаимный интерес деятельности, связанной с безопасностью, стабильностью и отказоустойчивостью. Сотрудники ICANN будут стремиться заручаться мнением РИР относительно конкретных совместных

проектов, требующих расширения с целью обеспечения безопасности, стабильности и отказоустойчивости DNS. Эти дискуссии будут в том числе направлены на понимание намерений РИР относительно возможных злоупотреблений наследием адресного пространства IPv4 и потенциальной необходимости формулирования глобальной политики для решения выявленных проблем.

## 6.4 Корпоративная безопасность ICANN и операции по непрерывности

6.4.1 Сотрудники ICANN обеспечат реализацию программ безопасности в рамках общих программ управления корпоративным риском, управления кризисными ситуациями и программ непрерывности деятельности. Основное внимание будет уделено устройству крепкого фундамента задокументированных планов и вспомогательных процедур. Конкретные инициативы по улучшению управления ситуации в ICANN относительно риска и непрерывности до середины 2010 годов включая оформление планов деловой непрерывности ICANN и управления кризисами, а также проведение внутренних учений в ICANN в совокупности с прочими проектами, подразумевавшим упражнения по поддержанию непрерывности рДВУ и подготовке конференций. В рамках реализации непрерывности ИТ ICANN улучшит использование альтернативных площадок. Для поддержки программ непрерывности ICANN будут предприняты массовые усилия и создан безопасный ИТ-центр и мощности для резервного копирования. В планы ICANN входит произвести оценку риска безопасности предприятий к середине 2009 года.

6.4.2 В течение следующего года сотрудники ICANN обеспечат наличие полного спектра информации, кадров и механизмов безопасности во всех сферах её деятельности. Как и в случае с управлением риском и планированием непрерывности, основное внимание будет привлечено к образованию прочного основания для задокументированных планов и процедур поддержки. Среди конкретных инициатив по улучшению восприятия роли ICANN в течение середины 2010-го года будет использоваться улучшение логических и физических средств контроля и доступа, процесс обучения и повышения осведомлённости сотрудников, план безопасности для путешествующих, планирование

безопасности совещаний и реагирования. ICANN берёт на себя обеспечение взаимодействия с развивающимся сообществом, развитие и реализацию ИТ-инструментов по повышению осведомлённости при наличии адекватных контролей безопасности.

6.4.3 Сотрудники ICANN планируют работать с Институтом программных технологий (ИПТ) при Университете Карнеги-Меллона по использованию технологической структуры отказоустойчивости (ТСО) ИПТ для обеспечения использования передового опыта в программах безопасности, непрерывности и управления риском и измерения изменений на постепенном пути к полноценному развитию. К концу 2009 г. ICANN планирует завершить оценку степени развития своего основного процесса в соответствии с подходом ИПТ. Кроме того, ICANN планирует провести внешний анализ своих программ безопасности и продолжительности, осуществлявшихся за первую половину 2010 г.

## 6.5 Организации поддержки и консультативные комитеты ICANN

6.5.1 ККБС планирует сосредоточить свои усилия в будущем на развёртывании DNSSEC, защите регистрации доменов и сокращении неправомерного использования доменных имён и стабильности системных адресов.

6.5.2 В январе 2009 г. Совет ОПРИ выставил на открытое обсуждение и для принятия Советом дальнейших решений *предварительный отчёт по хостингу «Fast Flux»* и также рассматривает многочисленные возможные сопутствующие исследования Whois. При Совете ОПРИ создана рабочая группа, посвящённая второму из шести проектов разработки политики, направленному на различные аспекты изменения регистраторов. ОПРИ создала рабочую группу по вопросам злоупотреблений при регистрации и рассматривает инициативу, связанную с восстановлением доменных имён после истечения срока их действия. С целью собрать вместе широкий круг субъектов ICANN, заинтересованных в данных вопросах, на 34-ой международной открытой конференции ICANN в Мехико в марте 2009 года прошёл расширенный семинар по электронным преступлениям, а также семинар, полностью посвящённый исключительно вопросу злоупотреблений при регистрации.

## 6.6 Международная деятельность

### 6.6.1 Расширение существующих партнёрств

Суть стратегии глобальной деятельности ICANN в отношении безопасности, стабильности и отказоустойчивости заключается в том, чтобы развивать и использовать существующие результаты работы, осуществляемой отделом глобальных партнёрств и ещё более расширять крепкие партнёрские отношения. На 2010-ый финансовый год с этими партнёрами запланированы следующие проекты.

- ***Общество Интернета (ISOC)*** – ICANN планирует продолжать сотрудничество в рамках продолжающейся совместной программы ISOC и ICANN по обеспечению образовательных курсов для операторов ДВУ, а в дополнительные планы входит техническое обучение методам повышения безопасности, сокращения последствий кибер-атак и сбоев.
- ***DNS-ОАИЦ*** – ICANN поддержит формирование контролируемого DNS-ОАИЦ портала для обмена информацией и передовым опытом в области безопасности, стабильности и отказоустойчивости в рамках сообщества ДВУ. ICANN также взаимодействует с различными организациями по проведению образовательных мероприятий, нацеленных на улучшение понимания работы систем уникальных идентификаторов, роли корпорации и трудностей, возникающих при управлении рисками для этих систем.
- ***Азия*** – ICANN планирует рассмотреть сотрудничество с новым международным центром кибербезопасности, поддерживаемым правительством Малайзии, сосредоточенном на том, как ICANN может вносить свой вклад в международные усилия по борьбе со зловредными кибердействиями, способными угрожать системам уникальных идентификаторов Интернета.

### 6.6.2 Коммерческие предприятия

ICANN будет развивать результаты прошедшего в феврале 2009 г. симпозиума по безопасности, стабильности и отказоустойчивости DNS в области понимания зависимости предприятий и рисков, связанных с DNS. В будущем году усилия в сфере безопасности, стабильности и отказоустойчивости войдут в программу разъяснительной деятельности генерального директора ICANN с целью объединения как можно более широкого ряда корпоративных перспектив.

### 6.6.3 Участие в международном диалоге по кибербезопасности

ICANN будет принимать участие в данных диалогах с целью формирования чёткого понимания своей конкретной роли и вклада. В этой сфере ICANN готовит на следующий год следующие проекты.

- ***Центр стратегических и международных исследований (ЦСМИ)*** – ICANN планирует провести серию совместных семинаров в 2009-2010 гг., на которых, в том числе, будет обсуждаться вопрос организации с многочисленными субъектами в обеспечении глобальной кибербезопасности. В рамках этих совместных усилий совместные семинары с партнёрскими институтами ЦСМИ будут проведены и за пределами США.
- ***Атлантический совет*** – ICANN планирует сотрудничать с Атлантическим советом по проектам, связанным с борьбой с растущей уязвимостью малых стран и организаций в свете расширения кибер атак и протестов. ICANN сосредоточит внимание на своей роли по обеспечению отказоустойчивости DNS под напором таких воздействий.

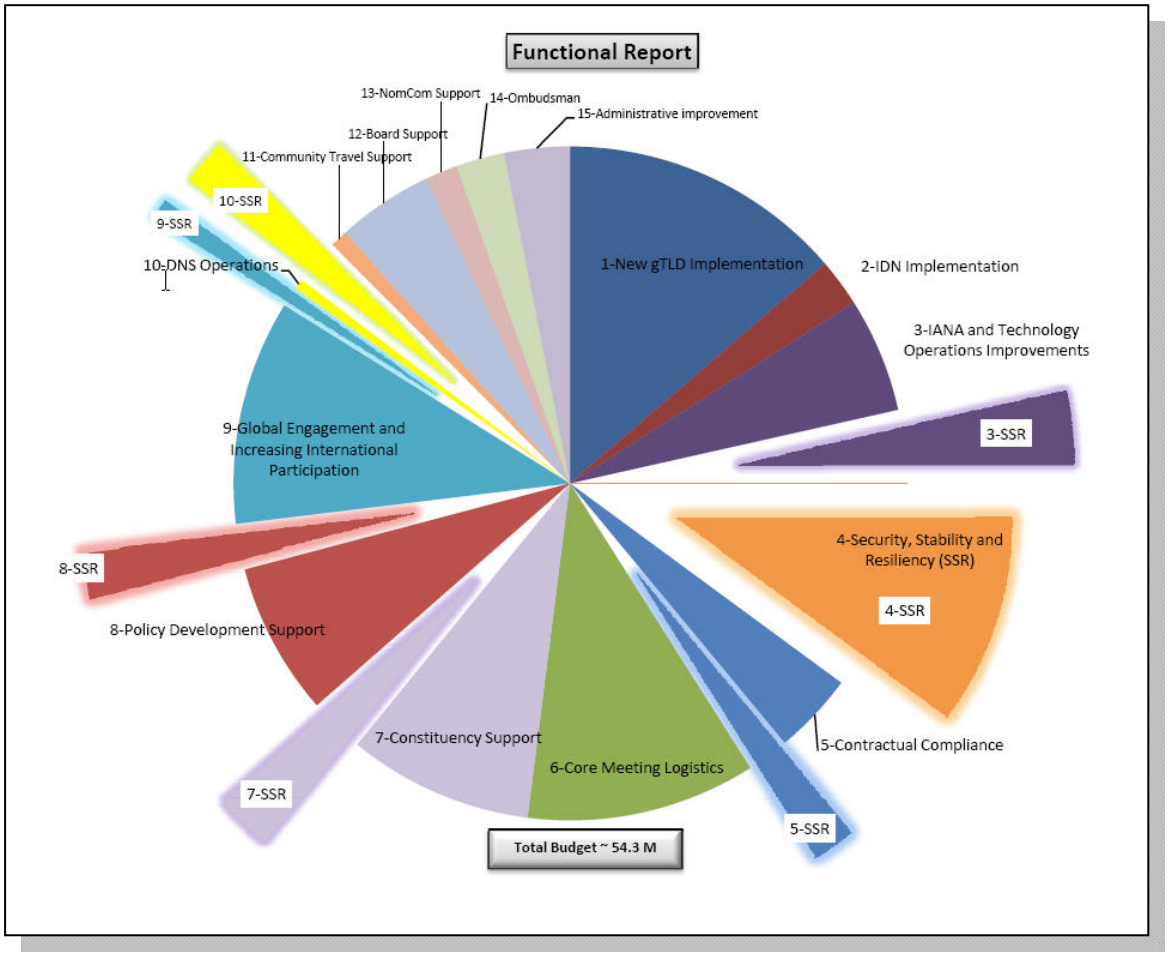
ICANN будет активно преследовать возможности для сотрудничества с другими научно-исследовательскими центрами и высшими учебными заведениями для развития передовых идей по решению задач, связанных с безопасностью, стабильностью и отказоустойчивостью.

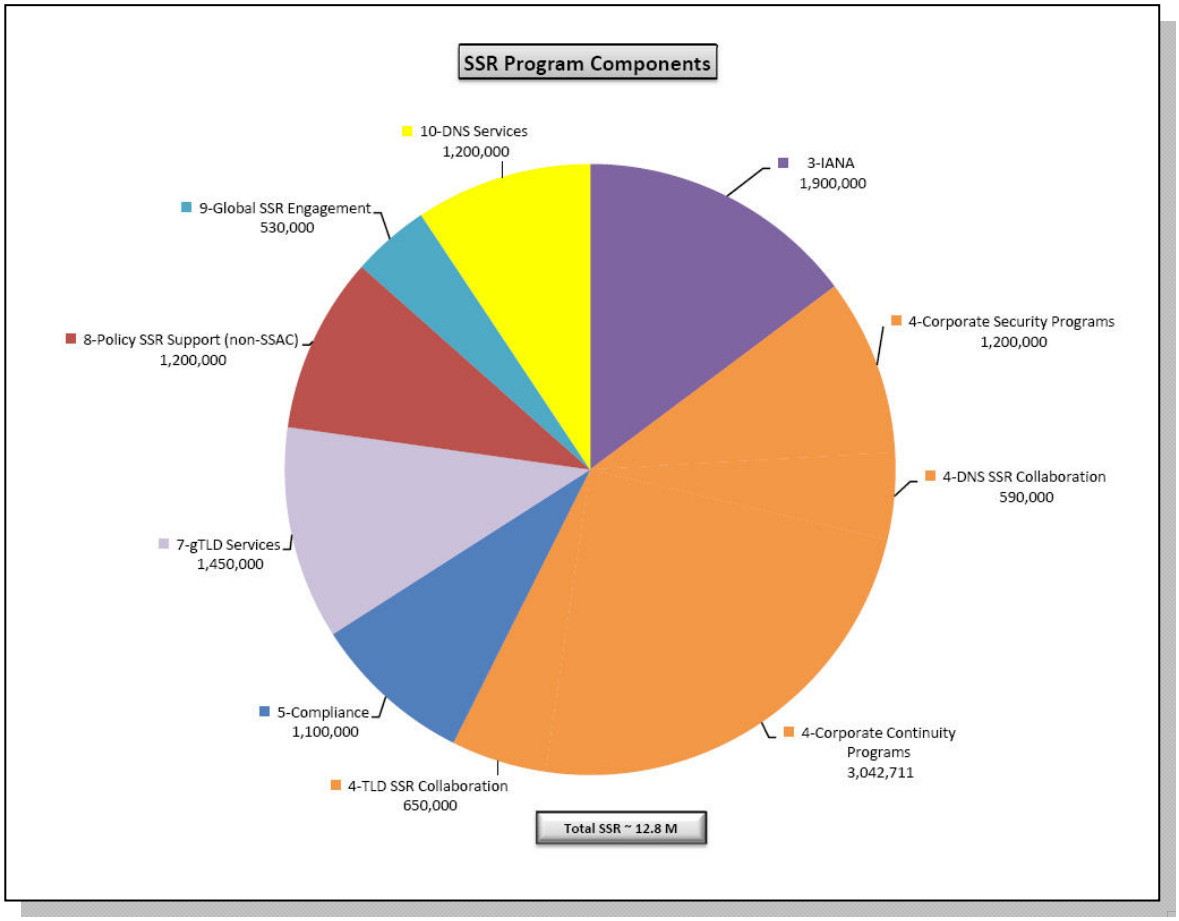
# 7. Заключение

ICANN осознаёт, что ключевым аспектом её задачи по формированию доверия общественности является вклад её программ и проектов в превращение систем уникальных идентификаторов в ключевой аспект более безопасной, стабильной и отказоустойчивой Интернет-среды. Трудности растут, и усилия ICANN в этом направлении становятся всё более напряжёнными. ICANN также признаёт ограничения своей рои и ресурсов и планирует свою стратегию в этой сфере с упором на сотрудничество. Интернет представляет собой глобальную среду, в которой координирование разнообразных субъектов позволяет стимулировать инновации. Вклад ICANN в укрепление безопасности, стабильности и отказоустойчивости её систем уникальных идентификаторов будет полагаться на тот же подход.

С момента своего создания ICANN осуществляет программы и проекты, направленные на улучшение безопасности, стабильности и отказоустойчивости Интернета, включая усилия, связанные с ключевыми функциями DNS и адресной системы; сотрудничество с сообществами реестров и регистраторов ДВУ; взаимодействие с ОНР и РИР; программы корпоративной безопасности и непрерывности; деятельность организаций поддержки и консультативных комитетов, участие в глобальных и локальных проектах по безопасности, стабильности и отказоустойчивости Интернета. Задачей первого проекта плана является обеспечить основание для развития роли ICANN и структуры, вокруг которой корпорация бы организовала свои усилия в сфере безопасности, стабильности и отказоустойчивости. План будет развиваться со временем как часть процесса стратегического и операционного планирования ICANN, позволяя проектам корпорации сохранять актуальность и обеспечивать применение её ресурсов на выполнение наиболее важных обязанностей и вкладов.

# Приложение А




SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
4-Corporate Security Programs
1,200,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
5-Compliance
1,100,000
4-Corporate Continuity
Programs
3,042,711
4-TLD SSR Collaboration
650,000
Total SSR ~ 12.8 M

## Overview of Major Components of ICANN Security, Stability, Resiliency (SSR) Program

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K

**OVERALL SSR – $12.8 M**

- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $3.0 M
- Policy SSR Support (incl SSAC) - $1.2M

## **IANA Security, Stability and Resiliency** (IANA)

| Objectives | Deliverables (milestones) |
|---|---|
| - Automation of key elements in root zone change process<br>- DNSSec operational readiness<br>- Test rPKI implementation<br>- Business continuity | - Implementation of automated RZM (date depends DOC approval; plan to have ready prior to implementation of new gTLDs)<br>- Implement DNSSec signing of .ARPA (date depends on coordination with IAB and DOC)<br>- Coordination with rPKI testers (currently underway)<br>- IANA Continuity & Disaster Recovery Plan (approved by August 2009) |
| **Key Stakeholders** | **Resources** |
| - IANA, Security, IT<br>- DOC/USG; Verisign<br>- SSAC; RSSAC<br>- IETF; DNS operator community, RIR communities; NRO | - Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support)<br>- Financial – $1.9M to support FTEs; staff support/travel; professional services; application development |

## **ICANN DNS Services** (IT Services)

| Objectives | Deliverables (milestones) |
|---|---|
| - Prepare for DNSSEC zone signing for ICANN zones, ARPA-related zones and the root<br>- Implement Trust Anchor Repository (TAR)<br>- Secure, resilient L-root operation | - Trust Anchor Repository in full production: June 09<br>- L-root improvement (new design deployed at LA and Miami, 3rd node deployed at Prague): June 09<br>- Production infrastructure in place for signing root zone: Oct 09<br>- DNSSec signed ICANN zones: Oct 09 |
| **Key Stakeholders**<br>- ICANN IT Services Team<br>- ICANN IANA staff, DoC, VeriSign<br>- ICANN Security & Resiliency Team | **Resources (FY 10)**<br>Human – 7.0 FTE (including related IT and other staff support)<br>Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel |

## **ICANN gTLD Registry/Registrar Services** (Services)

| Objectives | Deliverables |
|---|---|
| - Ensure implementation new gTLD/IDNs addresses SSR issues<br>- Continue maturing data escrow process & gTLD continuity procedures<br>- Conduct RSEP/RSTEP processes on registry services proposals | - Enhanced gTLD implementation process from SSR perspective<br>  - SSAC/RSSAC study complete (Fall 09)<br>  - Improved applicant guidebook (Aug 09)<br>- Conduct data escrow test (Aug-Sep 09 or Jan 10)<br>- Community failover exercise (Jan 10)<br>- RSEP/RSTEP studies as required |
| **Key Stakeholders**<br>- Registries/Registrars<br>- ICANN Services staff<br>- ICANN Security & Continuity staff<br>- GNSO/SSAC | **Resources (FY 10)**<br>Human – 2.75 FTE<br>Financial – $1.45M includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support |

## Contractual Compliance (Services)

| Objectives | Deliverables |
|---|---|
| - Improved ICANN compliance process<br>- Improved compliant and WDPRS system<br>- Improved WHOIS data accuracy | - Conduct audits as part of revised RAA implementation (50-100 by summer 2010)<br>- Reporting improvements to WDPRS (by June 2010)<br>- Conduct WHOIS related studies to further understanding of systems<br>  - Proxy usage (Oct 2009)<br>  - Data accuracy (Dec 2009) |
| **Key Stakeholders**<br>- gTLD registry/registrars<br>- ICANN Compliance staff<br>- ICANN Security/Continuity staff | **Resources (FY 10)**<br>Human – 3 FTE<br>Financial – $1.1M support for FTEs, staff/travel support; professional services to conduct studies and support systems improvements |

## TLD Security, Stability & Resiliency Collaboration

(Security)

| Objectives | Deliverables (milestones) |
|---|---|
| - Mature Attack & Contingency Response Program<br>- Establish joint ISOC/ICANN tech training program<br>- Establish TLD exercise planning workshops<br>- Establish program metrics | - Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09)<br>- Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009)<br>- Conduct exercise planning workshops (initial implementation Oct 2009)<br>- Prototype metrics based on Resiliency Engineering Framework (fall 2009) |
| **Key Stakeholders**<br>- ccTLD operators<br>- ccNSO, regional TLD operators<br>- ISOC/NSRC<br>- ICANN staff | **Resources (FY 10)**<br>Human – 1 FTE<br>Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs |

## DNS Security, Stability & Resiliency Collaboration

(Security)

| Objectives | Deliverables (milestones) |
|---|---|
| - Establish collaborative response mechanisms to DNS abuse<br>- Share key SSR practices<br>- Conduct community-based DNS risks & collaboration symposium<br>- Enhance root server SSR collaboration | - Collaboration construct and on-going responses w/ partners (construct in place summer 2009)<br>- Info Sharing Portal (Dec 09)<br>- Conduct & report on symposium (Feb & Mar 2010)<br>- Co-sponsor joint root community communications exercise (Fall 2009) |
| **Key Stakeholders** | **Resources (FY 10)** |
| - ISOC, DNS-OARC, FIRST<br>- Root Server community<br>- Broader DNS ops community<br>- ICANN staff<br>- RSSAC/SSAC | Human – 1.25 FTE<br>Financial – $590K for FTE, professional services for portal and collaboration support, travel to support activities |

## Corporate Security Program (Security, IT, others across staff)

| Objectives | Deliverables |
|---|---|
| - Improve and implement IT/Facilities/ Personnel Security Programs<br>- Establish Formal Plans<br>- Institute Security Training<br>- Implement Traveler and Meetings Security & Contingency Plans | - Conduct Security Training Programs (embedded part of ICANN on-boarding by Sep 2009)<br>- Improved IT & Physical Access Control Systems implemented (improved IT authentication on key systems – Fall 09)<br>- Exercise Traveler and Meetings Security (one drill per trimester) |
| **Key Stakeholders** | **Resources** |
| - ICANN Security & Resiliency Team<br>- ICANN IT/IANA/DNS Ops<br>- ICANN Human Resources<br>- ICANN Global Meetings Team<br>- Other ICANN Staff | Human – 2 FTEs (includes IT support for security)<br>Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits |

## Corporate Continuity Program (Security, IT, others across staff)

### Objectives

- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs

### Deliverables

- Initial ICANN Business Continuity plan (Oct 09)
  - Improved Crisis Management plan (Aug 09)
- Establish Secure IT Data Center (Sep 09)
- Exercise Business Continuity/Crisis Management (Spring 10)

### Key Stakeholders

- ICANN Security & Resiliency Team
- ICANN IT/IANA/DNS Ops
- ICANN Human Resources
- ICANN Global Meetings Team
- ICANN Staff

### Resources

Human – 5 FTEs (includes planning and IT for data center)

Financial – $3.0M including FTEs, capital support for data center, professional services for conducting training and audits

## Global Security, Stability and Security Engagement

(Global Partnerships & Security)

### Objectives

- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council)
- Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others)
- Collaborate with others on global cyber security response

### Deliverables

- Conduct joint activities with partner organizations (One per trimester)
- Engagement in forums across all major regions (On-going)
- Engage with Forum of Incident Response and Security Teams regarding ICANN role in response (initial findings Jan 2010)

### Key Stakeholders

- Global/international organizations
  - ISOC; IETF; ITU; IGF
- Cyber security forums
- Governments/Commercial Stakeholders
- ICANN Global Partnerships Team & Security Staff

### Resources (FY 10)

Human – 1.5 FTE

Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development

**Policy Support for SSR-related efforts incl. SSAC** (Policy)

| Objectives | Deliverables |
|---|---|
| Set by supported SO/Acs conducting SSR activity<br>- GNSO; ccNSO<br>- GAC<br>- SSAC<br>- RSSAC; ALAC | - SSAC Reports, Advisories, Comments<br>- Domain name protection study (Jun 09)<br>- Root Scaling Study with RSSAC (Sep 09)<br>- Others will depend on SO/AC FY 10 work plans |
| **Key Stakeholders**<br>- Named SO/Acs<br>- Названные ОП и КК<br>- ОПА<br>- Сотрудники | **Resources (FY 10)**<br>Human – 3.5 FTE<br>Financial – $1.2M for FTEs and limited additional funding support for SSR-related activities; support for SSAC/RSSAC root scaling study |

# Приложение B – Глоссарий терминов и сокращений, используемых в плане БСО

**ПРНЧП –** планирование реагирования на нападения и чрезвычайные происшествия

**Дополнительный льготный период –** пятидневный льготный период с момента регистрации регулируемого ICANN домена второго уровня. Владелец регистрации имеет право отменить регистрацию в течение этих пяти дней, при этом регистрационный взнос полностью возмещается реестром доменных имён.

**РГБФ –** рабочая группа по борьбе с фишингом

**НАС –** номера автономной системы: в Интернете автономная система (АС) – это набор связанных префиксов IP-маршрутирования, обеспечивающий единую, чётко определённую политику маршрутирования в Интернет. Провайдеры Интернет-услуг (ISP) должны официально зарегистрировать номер автономной системы (НАС) в IANA.

**ОПНИ –** организация поддержки национальных имён ICANN является органом разработки политики по узкому кругу вопросов, связанных с национальными доменами верхнего уровня, на глобальном уровне в рамках структуры ICANN.

**нДВУ –** национальный домен верхнего уровня

**CENTR –** совет европейских реестров национальных доменов верхнего уровня представляет собой ассоциацию реестров национальных доменов верхнего уровня, таких как .uk в Великобритании и .es в Испании. Полное членство доступно организациям, юридическим или физическим лицам, являющимся операторами реестра домена верхнего уровня.

**ЦСМИ –** центр стратегических и международных исследований предоставляет консультации по стратегическим вопросам и решения в области политики лицам, ответственным за принятие решений, в правительствах, международных организациях, частном секторе и гражданском обществе.

**ФББРБ –** форум бригад быстрого реагирования и безопасности

**рДВУ –** родовой домен верхнего уровня

**IANA —** агентство по распределению номеров Интернета

**ИДИ —** интернациональные доменные имена

**IETF —** комиссия по технологиям Интернета

**IP –** Интернет-протокол, указывающий формат пакетов и схему обращения по адресам. В большинстве сетей IP сочетается с протоколом более высокого уровня под названием протокол контроля передачи (Transmission Control Protocol, TCP), устанавливающим виртуальную связь между точкой назначения и источником. По сути IP является чем-то наподобие почтовой системы. Он позволяет Вам направить пакет и выслать его через систему, но прямая связь между Вашим пакетом и получателем отсутствует. TCP/IP устанавливает связь между двумя хостами, позволяя им обмениваться сообщениями.

**IPv4 –** четвёртая версия Интернет-протокола – это четвёртое поколение в развитии Интернет-протокола (IP) и первая версия, получившая широкое распространение. Совместно с IPv6 он лежит в основе методов соединения сетей Интернета на основе стандартов и продолжает оставаться наиболее широко распространённым протоколом межсетевого уровня.

**IPv6 –** шестая версия Интернет-протокола – это протокол межсетевого уровня следующего поколения для сетевых комплексов с пакетным коммутированием и Интернета. Комиссия по технологиям Интернета (IETF) разработала IPv6 в декабре 1998 г. в качестве преемника четвёртой версии, опубликовав спецификацию стандарта RFC 2460.

**ISOC —** общество Интернета

**ИТ –** информационные технологии

**Бот-сети** – чаще всего создаются, обманным путём заставляя обычных пользователей открывать приложения на своих компьютерах, которые на первый взгляд ничего не делают, но, на самом деле, устанавливают скрытое ПО, которое позже используется для нападения. Заражённые компьютеры или «боты» соединяются в сети, которыми затем можно управлять по желанию, чаще всего для злоумышленных нападений.

**Отравление кэш** – использование недостатка ПО DNS, чтобы заставить её принять неверную информацию, из-за которой сервер затем заносит в кэш-память неверные данные и направляет все последующие запросы сервера на новый домен с фальшивой верификацией.

**Атака типа «отказ в обслуживании» (DoS)** – зловредный код, вызывающий поток входящих сообщений, по сути заставляющий целевую систему отключиться, блокируя таким образом доступ для легитимных пользователей.

**Распределённая атака типа «отказ в обслуживании» (DDoS)** – подвид атаки типа «отказ в обслуживании», при котором злоумышленник использует зловредный код, установленный на нескольких системах для нападения на одну цель. Этот метод наносит больший вред цели, чем было бы возможно всего с одной атакующим компьютером. В Интернете распределённая атака типа «отказ в обслуживании» – это атака, при которой множество заражённых систем нападают на единую цель, вызывая отказ в обслуживании пользователей системы, подвергшейся нападению. Поток входящих сообщений, по сути, заставляет целевую систему отключиться, блокируя таким образом доступ для легитимных пользователей. Атаки DDoS наносят наибольший урон, когда их запускают с большого количества открытых серверов рекурсивного типа: распределение увеличивает трафик и сокращает возможность выявить источники нападения. Воздействие на открытые рекурсивные серверы обычно невелико, в то время как воздействие на цель очень значительно. Фактор амплификации оценивается около 1:73. Атаки, основанные на данном методе, достигали 7 Гигабит в секунду.

**DNS –** система доменных имён, переводящая доменные имена (состоящие из символов) в IP-адреса (цифровые). В целях простоты запоминания доменные имена представлены символами. Сам Интернет, однако, основан на цифровых IP-адресах (например 198.123.456.0). Когда Вы используете доменное имя (www.examplir.gratis.com), одна из служб DNS переводит имя из символов в соответствующий цифровой IP-адрес.

**DNSSEC** – расширения безопасности системы доменных имён позволяют программному обеспечению подтвердить, что данные системы доменных имён (DNS) не были изменены при передач через Интернет. Это обеспечивается включением в DNS пары открытый-закрытый ключ подписи для формирования цепочки доверия, создаваемой в корневой зоне. Важно отметить, что DNSSEC не является разновидностью шифрования. Наоборот, технология полностью совместима с существующей DNS; записи остаются в первоначальном виде — незашифрованными. Неприкосновенность записей обеспечивается использованием цифровых подписей, которые подтверждают их подлинность.

В основе DNSSEC заложена концепция «цепочки доверия». Предложение ICANN по подписанию файла корневой зоны при помощи DNSSEC (от октября 2008 г.) построено на этой идее и консультациях по безопасности, рекомендующих, чтобы субъект, отвечающий за выполнение изменений, дополнений и удалений в файле корневой зоны и подтверждающий действительность этих изменений, создавал и подписывал итоговый вариант файла

корневой зоны цифровым способом. Подписанный файл затем должен быть отправлен для распределения в другую организацию (в данный момент в корпорацию VeriSign). Другими словами, организация, отвечающая за первичную основу доверия, — утверждение изменений корневой зоны операторами доменов высшего уровня — должна также проверять правомочность конечного продукта до его распространения.

**Упреждённое использование доменных имён –** сомнительная практика, используемая некоторыми регистраторами доменных имён, использующих инсайдерские сведения для упреждающей регистрации доменных имён с намерением их продажи с накруткой регистрирующимся лицам, которые по логике могли бы извлечь прибыль от регистрации имени для собственного пользования.

**Пробное использование домена** – практика, при которой лицо, регистрирующее доменное имя, пользуется пятидневным дополнительным льготным периодом непосредственно после регистрации регулируемого ICANN домена второго уровня, чтобы протестировать успех на рынке доменного имени. В течение этого периода владелец регистрации проводит анализ экономической эффективности и возможности извлечения дохода из рекламы, размещаемой на веб-сайте домена.

Пробное использование домена не следует путать с **подделкой домена**, представляющей из себя механизм удаления доменного имени в течение пятидневного периода пробного использования и немедленной повторной регистрации на ещё один пятидневный период. Этот процесс повторяется n-ное количество раз, фактически обеспечивая постоянную бесплатную регистрацию домена.

**Double flux** – особую обеспокоенность у ICANN вызывает разновидность «fast flux», называемая «double flux», при которой злоумышленник меняет не только адреса, направляющие на незаконные веб-сайты, но и адреса именных серверов DNS, которые он использует, на «удобные для пользователей» имена, содержащиеся в фишинговых сообщениях по электронной почте. В обоих случаях изменения происходят очень быстро (занимаю порядка трёх минут), что практически не оставляет эксперта времени на реагирование. ККБС ICANN тесно сотрудничает с организациями по защите торговых марок и правоохранительными органами, равно как и с реестрами и регистраторами, над выявлением контр-мер, в особенности предотвращающих использование DNS в процессе «fast flux».

**Fast flux** – техника ухода от обнаружения, используемая фишерами, мошенниками, использующими чужие личные

данные, и прочими электронными преступниками, для противодействия усилиям бригад реагирования на нападения и правоохранительных органов по отслеживанию и закрытию противозаконных веб-сайтов. Техника «fast flux» сильно напоминает игру в «напёрстки», в которой мошенник кладёт три согнутые карты на стол, а жертву обманом заставляют ставить на своё умение «найти красную даму» (в Британии этот вид шулерства так и называется: «найди даму»). Мошенник с ослепительной скоростью двигает все три карты, отвлекая, при этом, жертву разговором, остроумными замечаниями и мановениями рук. Однако «Fast flux» – это трюк с высокими ставками, превратившийся в повсеместно используемый и вызывающий особое беспокойство способ нападения. Суть хостинга «fast flux» заключается в том, что мошенник быстро меняет адреса, направляющие на нелегальные веб-сайты.

**Зловредное ПО –** английское название этих программ, «malware», происходит от слияния слов «malicious» (зловредный) и «software» (программное обеспечение); под этим термином зачастую понимаются компьютерные вирусы, вирусы-черви, трояны, руткиты, шпионское ПО, рекламное ПО, преступное ПО и любое прочее нежелательное ПО, устанавливаемое на компьютере пользователя без его согласия. Зловредное ПО считается таковым, скорее, на основании воспринимаемого намерения его создателя, чем на основе каких-то конкретных характеристик программ.

**ЦСО** – центр сетевых операций – это физическое место, с которого обычно осуществляется управление, контроль и надзор за крупной сетью. ЦСО также обеспечивают подключение к сети для пользователей, подсоединяющихся к сети извне физического пространства.

**ГОС –** группа операторов сетей

**ОНР –** организация номерных ресурсов

**Патчи** – программы, нацеленные на исправление недостатков в ПО; часто устанавливаются автоматически, чтобы сократить необходимость вовлечения конечного пользователя и упростить пользование.

**Фишинг** – форма Интернет-мошенничества, направленная на кражу ценной информации, как например, номера кредитных карт и социального страхования, пользовательские имена и пароли, путём создания веб-сайта, похожего на сайт легитимной организации и направления потоков электронной почты на поддельный сайт с целью сбора конфиденциальной информации для извлечения финансовой или политической выгоды.

**САР –** соглашения об аккредитации регистраторов.

**Реестр –** организация, занимающаяся регистрацией мён доменов верхнего уровня Интернета.

**Регистратор –** компания, имеющая разрешение на регистрацию доменных имён Интернета.

**РИР —** региональный Интернет-реестр.

**КОИр –** ключевая открытая инфраструктура ресурсов.

**ПОУР –** процесс оценки услуг реестра.

**ГТОУР –** группа технической оценки услуг реестра.

**Спам** – любые непрошеные непрошенные сообщения электронной почты. Хотя обычно он рассматривается просто как дорогостоящий раздражитель, в наши дни спам часто содержит зловредное ПО. Зловредное ПО – это программное обеспечение: вирусы, черви, трояны и шпионское ПО, – целью которого является инфицировать компьютеры и системы для кражи ключевых сведений, удаления приложений, дисков и файлов или обращения компьютера в инструмент для преступника извне.

**Спуфинг** – вид нападения, при котором лицо или программа выдают себя за других путём подделки данных. Подделанные данные принимаются как верные отдельными системами, пытающимися подключиться к легитимной системе или программе.

**ДВУ –** домен верхнего уровня.

**Троян –** класс зловредного ПО, которое на первый взгляд выполняет желаемую функцию, а вместо этого осуществляет зловредные функции, открывая недозволенный доступ к машине-хосту, позволяя пользователям трояна сохранять свои файлы на компьютер ничего не подозревающего пользователя, или даже наблюдать за экраном пользователя и контролировать его компьютер.

**Вирус** – программа или строка кода, загружаемая на компьютер без ведома пользователя и запускающая зловредное ПО. Даже простейший вирус способен самовоспроизводиться, что делает его ещё более вредоносным, так как он быстро использует всю имеющуюся оперативную память на инфицированной компьютерной системе.

**Вирус-червь –** схож с вирусом по природе; червь считается разновидностью вируса, но несёт большую опасность по причине его способности самораспространяться в сети. Черви переносятся

с компьютера на компьютер, но в отличие от вирусов, они способны перемещаться без намеренного или ненамеренного участия человека. Червь использует функции переноса файлов или информации в компьютерной системе, что позволяет ему путешествовать без посторонней помощи. К примеру, червь может отправить свою копию при помощи адресной книги электронной почты пользователя. Затем он размножается на инфицированных компьютерах и снова распространяется через записные книги электронной почты в новых инфицированных системах; он продолжает поглощать оперативную память, по не занимает столько памяти и пропускной способности, что способен остановить работу целых сетей.