План повышения безопасности, стабильности и отказоустойчивости Интернета (2011 ФГ)

Сентябрь 2010 г.

Содержание

Сводное резюме

Интернет представляет собой успешную экосистему, в которой разнообразные заинтересованные стороны организованы на основе сотрудничества, направленного на стимулирование общения, творчества и торговли в общей 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 сохранение и повышение безопасности, стабильности и отказоустойчивости этих систем является ключевым элементом их сотруднических отношений.

Настоящий документ является обновлением плана ICANN по повышению безопасности, стабильности и отказоустойчивости Интернета, опубликованного 16 мая 2009 года (именуемого в дальнейшем «план по БСО на 2009 год», http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf). План по БСО на 2011 ФГ был обновлен с целью отражения в нем деятельности ICANN в сфере безопасности за период с июня 2010 года по июль 2011 года. Обновления плана по БСО на 2009 год выделены курсивом. План по БСО на 2011 ФГ публикуется для сбора комментариев в период с августа по сентябрь 2010 года.

В стратегическом плане ICANN на 2010–2013 годы (http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf) содержится следующая формулировка. «Стабильность и безопасность системы доменных имен (DNS) является важным приоритетом для сообщества ICANN и пользователей Интернета в целом. Это ключевые элементы миссии ICANN. Интенсивность злоупотреблений DNS и атак на эту систему и другие компоненты инфраструктуры Интернета неуклонно возрастает. Для обеспечения безопасности, стабильности и отказоустойчивости, являющихся критически важными для DNS, ICANN должна сотрудничать с другими субъектами, принимающими участие в решении широкого спектра указанных вопросов.»

[1] Согласно уставу ICANN корпорация координирует распределение и назначение трех комплектов уникальных идентификаторов для Интернета: доменные имена, формирующие систему DNS; адреса интернет-протокола (IP)и номера автономной системы (AC); а также номера портов протоколов и параметров.

В стратегическом плане стабильность и безопасность DNS указаны в качестве одной из четырех важнейших стратегических сфер приложения усилий ICANN. Это соответствует высокой важности, которая придается БСО в Подтверждении обязательств (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm), подписанном 30 сентября 2009 г. ICANN и Национальным управлением по телекоммуникациям и информации США (NTIA). Широкий диапазон обязанностей ICANN по обеспечению безопасности, стабильности и отказоустойчивости разделен на стратегические задачи, работу сообщества, стратегические проекты и работу персонала.

Безопасная, стабильная и отказоустойчивая работа системы уникальных идентификаторов Интернета является ключевой частью миссии ICANN. В свете увеличения частоты и изощренности агрессивных атак и других видов злонамеренного поведения корпорация ICANN и ее сообщество должны продолжать совместную работу, направленную на повышение отказоустойчивости DNS и укрепление ее возможности вести борьбу с такими атаками. По мере расширения разновидностей атак и злонамеренного поведения корпорация ICANN должна проводить работу с другими заинтересованными сторонами, направленную на разъяснение роли ICANN и поиск решений проблем, выходящих за рамки миссии любой отдельно взятой организации.

Стратегические задачи, сформулированные для обеспечения безопасности и стабильности DNS:

1. *Абсолютно безотказное функционирование DNS.*
2. *Сокращение злоупотреблений DNS.*
3. *Повышение безопасности операций с доменами верхнего уровня (ДВУ).*
4. *Повышение сопротивляемости DNS нападениям.*

12 февраля 2010 года ICANN опубликовала Предлагаемые стратегические инициативы по повышению безопасности, стабильности и отказоустойчивости (БСО) DNS (http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf). В этом документе представлено обоснование, важнейшие характеристики и предполагаемые расходы двух стратегических инициатив, относящихся к безопасности и стабильности DNS.

На основе комментариев, полученных в периоды двух общественных обсуждений, во время конференции ICANN в Найроби, проведенного в апреле 2010 года семинара по совместному анализу требований к функционированию DNS-CERT и конференции ICANN в Брюсселе, ICANN не планирует управлять DNS-CERT, а вместо этого продолжит работу по привлечению заинтересованных сторон к определению требований к функционированию объединенной системы реагирования на угрозы DNS, оценке рисков и анализу угроз в масштабах всей системы DNS.

Роль ICANN

ICANN руководствуется уставом корпорации при формировании политики, реализации процессов и программ (в том числе имеющих отношение к безопасности, стабильности и отказоустойчивости) с участием многих заинтересованных сторон на основе консенсуса.

- Роль ICANN должна в первую очередь относиться к ключевым задачам корпорации, связанным с системами уникальных идентификаторов.
- ICANN не выполняет роли правоохранительного органа Интернета по оперативному противодействию криминальной деятельности.
- ICANN не участвует в использовании Интернета для киберразведки и кибервойны.
- ICANN не участвует в определении составляющих противозаконного содержимого в Интернете.
- Роль ICANN включает участие в деятельности широкого интернет-сообщества по борьбе с неправомерным использованием систем уникальных идентификаторов. Такая деятельность подразумевает сотрудничество с правительственными структурами в борьбе со злонамеренным поведением, связанным со злоупотреблениями упомянутыми системами, и их защите.

Программы ICANN по обеспечению безопасности, стабильности и отказоустойчивости

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

- ICANN поддерживает усилия сообщества системы доменных имен (DNS) и адресации по укреплению основ безопасности, стабильности и отказоустойчивости этой системы. Эти усилия включают поддержку разработки и развертывания протоколов и вспомогательных технологий аутентификации имен и номеров Интернета.
- ICANN способствует организации мероприятий в сфере безопасности, стабильности и отказоустойчивости, проводимых реестрами DNS, регистраторами и прочими участниками сообщества.
- ICANN несет 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 повышения безопасности, стабильности и отказоустойчивости

В течение 2011 операционного года ICANN планирует реализовать программы и инициативы, изложенные в настоящем документе. В приложении A указаны конкретные цели, участники, результаты и ресурсные требования программ и мероприятий.

- ***Деятельность IANA*** *— 16 июля 2010 года ICANN, VeriSign и NTIA внедрили DNSSEC для достоверной корневой зоны. Это явилось существенным этапом повышения безопасности и стабильности Интернета. ICANN совместно с интернет-сообществом продолжит работу по устранению препятствий на пути внедрения DNSSEC. Прочие инициативы включают улучшение управления корневой зоной посредством автоматизации; улучшение методов аутентификации обмена информацией с управляющими ДВУ.*
- ***Операции корневых серверов DNS*** *—ICANN продолжит работу по планированию на случай возникновения непредвиденных обстоятельств и проведению учений с операторами корневой зоны, а также по улучшению отказоустойчивости и инфраструктуры корневого сервера «L».*
- ***Реестры рДВУ*** — оценка кандидатов на новые родовые домены верхнего уровня (рДВУ) и интернационализированные доменные имена (ИДИ) обеспечит дальнейшую безопасность деятельности.

ICANN продолжит добиваться принятия мер по борьбе со злонамеренным поведением в связи с созданием новых рДВУ. ICANN продолжит доработку плана бесперебойной работы реестров рДВУ и тестирование системы ответственного хранения данных.

- ***Реестры нДВУ*** *— по мере ввода нДВУ с ИДИ в рамках ускоренного режима ICANN продолжит усилия по решению вызывающих озабоченность вопросов, связанных с управлением вариантами и снижением рисков для безопасности.*

  ICANN продолжит свое сотрудничество с реестрами национальных доменов верхнего уровня (нДВУ) в рамках совместной программы планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП) и учебной программы по операциям реестра (ROC) во взаимодействии с Организацией поддержки национальных имен (ОПНИ), региональными ассоциациями доменов верхнего уровня (ДВУ) и Обществом Интернета (ISOC).

- ***Выполнение договорных обязательств*** — ICANN продолжит расширение масштабов деятельности по обеспечению выполнения договорных обязательств, связанных с рДВУ, и начнет проведение аудиторских проверок договорных сторон в рамках исполнения поправок к соглашению об аккредитации регистраторов (САР) от 2009 года и определение потенциальной возможности злонамеренного поведения договорных сторон для принятия исправительных мер. ICANN также продолжит содействие обсуждению политики в отношении мероприятий по обеспечению лучшего выполнения договорных обязательств в составе возможных поправок к САР в 2011 ФГ.

- ***Реагирование на умышленное злоупотребление DNS*** — ICANN продолжит развивать усилия по сотрудничеству и содействию обмену информацией для обеспечения эффективного реагирования на злонамеренное поведение, связанное со злоупотреблением DNS.

- ***Корпоративная безопасность ICANN и обеспечение непрерывности деятельности*** *— ICANN продолжит реализацию программ обеспечения безопасности в рамках общего управления корпоративными рисками и кризисными ситуациями, а также программ обеспечения непрерывности деятельности. Основное внимание будет уделено устройству крепкого фундамента в виде документально оформленных*

планов и вспомогательных процедур. Эти программы включают:

- ***Корпоративный план обеспечения информационной безопасности*** *— ICANN разработала корпоративный план обеспечения информационной безопасности, соответствующий стандартам ISO 27002. Этот план выполняется в 2011 ФГ.*
- ***План обеспечения безопасного проведения конференций*** *— в развитие усилий по поддержке более качественного планирования безопасности на всемирных конференциях ICANN был разработан план обеспечения безопасного проведения конференций, который будет использоваться при выборе места проведения и при подготовке к конференциям ICANN в 2011 ФГ и далее.*
- ***План обеспечения безопасности персонала и физических активов*** *— в рамках усилий по повышению безопасности персонала и объектов эти два плана реализуются в 2011 ФГ.*
- ***План обеспечения непрерывности деятельности и управления чрезвычайными ситуациями*** *— ICANN провела учения по непрерывности деятельности IANA в 2010 году, и эти усилия будут продолжены в 2011 ФГ путем проведения ICANN учений по связи в кризисной обстановке и реализации плана обеспечения непрерывности деятельности и управления чрезвычайными ситуациями.*
- ***Программа управления рисками предприятия*** *— ICANN внедрила Руководство по управлению рисками предприятия (УРП) и сформировала программу по УРП в 2010 ФГ. ICANN продолжит усовершенствование этой программы в 2011 ФГ, осуществляя оценку рисков и поддержку Комитета по вопросам рисков, созданного Правлением корпорации.*

- ***Обеспечение повсеместного участия и сотрудничества*** — ICANN продолжит расширение партнерских отношений с Комиссией по технологиям Интернета (IETF), Обществом Интернета (ISOC), региональными интернет-реестрами (РИР), группами операторов сетей (ГОС), операционным, аналитическим и исследовательским центром DNS (DNS-OARC) *и форумом групп быстрого реагирования (FIRST).* ICANN также будет принимать участие в межнациональных диалогах, направленных на расширение понимания трудностей в

сфере безопасности, стабильности и отказоустойчивости, стоящих перед экосистемой Интернета, и способов решения этих трудностей при участии большого количества субъектов.

1. Цель и обзор

В этом обновленном плане по БСО для широкого ряда заинтересованных сторон приводится описание того, 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 способы ее вовлеченности в эту сферу, приводится обзор существующих программ ICANN этой направленности и содержатся подробные сведения о запланированных мероприятиях и выделенных ресурсах на следующий операционный год. План состоит из семи разделов и приложения:

- Раздел 1. Цель и обзор
- Раздел 2. Трудности и возможности
- Раздел 3. Роль ICANN
- Раздел 4. Субъекты ICANN, принимающие участие в усилиях по обеспечению безопасности, стабильности и отказоустойчивости
- Раздел 5. Текущие программы ICANN, связанные с безопасностью, стабильностью и отказоустойчивостью
- Раздел 6. *Планы ICANN по повышению безопасности, стабильности и отказоустойчивости на 2011 ФГ*
- Раздел 7. Заключение
- *Приложение А. Цели, участники, этапы (результаты) и ресурсные требования программы ICANN по обеспечению безопасности, стабильности и отказоустойчивости на 2011 ФГ*

Как указано в сводном резюме, данный план разработан на основе плана по БСО на 2009 г. и развивает видение и задачи, описанные в стратегическом плане ICANN на 2010–2013 гг. Настоящая версия плана предназначена для дополнительного обновления основы, описывающей роль ICANN и ее сообщества, а также для расширения концепции корпорации по организации безопасности, стабильности и отказоустойчивости. Этот план был обновлен в рамках ежегодного пересмотра во взаимосвязи с циклами стратегического и оперативного планирования ICANN.

2. Трудности и возможности

Динамичной интернет-среде угрожает рост масштабов злонамеренной деятельности различного рода, включая интенсивное участие криминальных организаций в мошенничестве, вымогательстве и прочей незаконной деятельности онлайн, а также рост числа атак, вызывающих отказ в обслуживании, и прочей деструктивной деятельности, осуществляемой через Интернет. Деятельность в Интернете все в большей мере отражает полный спектр человеческих мотиваций и поведений. В прошлом такая деятельность отражала открытую природу Интернета, принесшую ему успех, позволила осуществлять передовые нововведения и способствовала общению, творчеству и торговле в глобальной среде. Однако открытость принесла с собой уязвимости. К примеру, растут случаи использования этих возможностей для «фабрикации» или «отравления» процесса разрешения DNS с целью 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. Полный спектр субъектов Интернета в течение нескольких последних лет выражает все возрастающую озабоченность: пользователи, предприятия, суверенные государства и организации, принимающие участие в обсуждении проблем Интернета, а также более широкое информационное сообщество. Усилия по решению этих трудностей должны быть также направлены против рисков для безопасности и стабильности, проистекающих из введения новых инструментов управления, которыми могут воспользоваться в своих интересах преступники, или архитектуры сетей, усложняющих обеспечение стабильности.

ICANN будет бороться с угрозами для безопасности, стабильности и отказоустойчивости Интернета в рамках своей сферы ответственности. В статье I устава ICANN указано, что миссия 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 трех 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 после них. ICANN сотрудничает с ответственными сторонами, представляющими различные элементы систем уникальных идентификаторов, для обеспечения ответственности за адекватную реализацию ее 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 четко определяя цели и параметры измерения эксплуатационных показателей при стратегическом, оперативном и финансовом планировании. Настоящий план обеспечивает сообщество ориентирами относительно путей выполнения ICANN своих обязанностей.

В приложении А к плану представлены подробности запланированных на 2011 ФГ действий, этапов и выделенных ресурсов. Основную долю внимания сотрудников отдела безопасности ICANN в 2011 ФГ будет занимать установление параметров для более объемных программ, нацеленных на улучшение общей безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов.

3. Роль ICANN

При формировании политики, реализации процессов и программ (в том числе имеющих отношение к безопасности, стабильности и отказоустойчивости) с участием многих заинтересованных сторон на основе консенсуса ICANN руководствуется уставом корпорации. Ключевая миссия ICANN заключается в обеспечении многосубъектного подхода к эффективному осуществлению функций IANA; установлении глобальных политик, обеспечивающих координацию DNS, адресацию через интернет-протокол (IP) и назначение IP-адресов; а также в стимулировании конкуренции и выбора в среде рДВУ посредством системы договоров с реестрами рДВУ и аккредитованными ICANN регистраторами.

Выполняя свою миссию, за последние десять лет ICANN сыграла определенную 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 отражен в системе договоров 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 скоординированной системы, направленной на сотрудничество.

ICANN планирует по-прежнему вносить свой вклад по ряду направлений с целью обеспечения безопасности, стабильности и отказоустойчивости систем адресации и имен Интернета в свете развивающихся рисков и угроз. При этом корпорация сосредоточит усилия на выполнении своей ключевой миссии, связанной с системами уникальных идентификаторов Интернета. Она не будет выступать в роли полицейского и не будет бороться с криминальной деятельностью злоумышленников на оперативном уровне. ICANN не занимается деятельностью, связанной с использованием Интернета для киберразведки 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.

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

- ICANN несет непосредственную ответственность за деятельность IANA и сотрудничает с Министерством торговли США и корпорацией VeriSign в области подготовки и распространения данных корневой зоны. Обеспечение безопасного, стабильного и отказоустойчивого функционирования корневой зоны DNS было и останется основным приоритетом. Кроме того, ICANN предоставляет основополагающие средства сообществу DNS и адресации, занимающемуся аутентификацией имен и номеров Интернета. ICANN убеждена, что важнейшим этапом в обеспечении безопасности DNS является внедрение расширений безопасности системы доменных имен (DNSSEC) (*ICANN, VeriSign и NTIA внедрили DNSSEC в корневой зоне 16 июля 2010 года*). Прочие важнейшие усилия сосредоточены на улучшении общесистемного понимания рисков, обеспечении внедрения единой отметки о доверии (ОД) в инфраструктуре открытых ключей ресурсов (ИОКР), а также на сотрудничестве с партнерами в области улучшения механизмов обеспечения безопасности и отказоустойчивости в рамках сообщества ДВУ.
- ICANN способствует организации мероприятий в сфере безопасности, стабильности и отказоустойчивости, проводимых реестрами DNS и регистраторами. Характер ролей и обязанностей ICANN зависит от конкретных характеристик ее взаимоотношений с этими ключевыми операторами. Наряду с совместной деятельностью ICANN поддерживает договорные отношения со всеми реестрами рДВУ и аккредитованными корпорацией регистраторами. Эти соглашения все в возрастающей мере становятся механизмами улучшения безопасности, стабильности и отказоустойчивости во всей DNS. Усилия ICANN по обеспечению соответствия требованиям и исполнению положений этих соглашений являются одним из ключевых элементов дальнейшего развития корпорации. В отношении реестров нДВУ ICANN и

операторы нДВУ выразили приверженность к дальнейшему повышению безопасности, стабильности и функциональной 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 также сосредоточит свои усилия на поддержке возможностей совместного реагирования сообщества в целях повышения безопасности DNS.

- ICANN принимает участие в деятельности Организации номерных ресурсов (ОНР) 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 несет прямую ответственность за безопасное, стабильное и отказоустойчивое функционирование своих собственных активов и служб при руководстве IANA и прочими координирующими функциями в качестве оператора корневого сервера «L» системы 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 атак до совместных усилий, направленных на противодействие злоумышленникам в Интернете, распространяющим вредоносные программы и занимающимся фишингом с использованием систем уникальных идентификаторов Интернета. К ним, например, относятся развернутые семинары по вопросам злоупотребления DNS и технологии DNSSEC, проведенные на последних конференциях ICANN.
- ICANN выполняет миссию доверительного фонда в свете ее роли координатора систем уникальных идентификаторов Интернета и берет на себя ведущую роль в решении трудностей, связанных с созданием безопасной, стабильной и отказоустойчивой экосистемы Интернета, которая при этом должна оставаться динамичной средой для глобального диалога, торговли и инноваций.

4. Субъекты ICANN, принимающие участие в усилиях по обеспечению безопасности, стабильности и отказоустойчивости

Участие ICANN в обеспечении безопасности, стабильности и отказоустойчивости включает деятельность самых различных сотрудников, организаций поддержки и консультативных комитетов корпорации. В число ключевых участников входят следующие субъекты.

- ***Действующий персонал IANA —*** отвечает за осуществление функций IANA, включая координацию корневой зоны DNS, функционирование реестра .arpa, распределение пространства IP-адресов и регистрацию параметров протоколов. Конкретные виды деятельности, связанные с обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.
- ***Оперативный персонал DNS*** — отвечает за операции в зоне КОРНЕВОГО СЕРВЕРА «L», одного из тринадцати корневых серверов имен, инфраструктуру DNSSEC для находящихся под управлением ICANN доменов и ДВУ, подписи DNSSEC КОРНЕВОЙ ЗОНЫ (KSK), средства KSK, церемонии и размещение нДВУ, полномочные серверы DNS, принадлежащие ICANN, и портфель доменов ICANN. Члены оперативной группы DNS вместе с другими участниками регулярно присутствуют на таких собраниях, как NANOG, RIPE, MENOG, LACNOG, NZNOG, SANOG, AFNOG, где обсуждаются различные аспекты проектов ICANN, имеющих отношение к функционированию DNS.
- ***Сотрудники отдела выполнения договорных обязательств и обязательств по обслуживанию*** — отвечают за обеспечение координации и выполнения соглашений реестрами рДВУ и аккредитованными ICANN регистраторами. Конкретные виды деятельности, связанные с обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.
- ***Сотрудники отдела политик*** — отвечают за содействие организациям поддержки и консультативным комитетам в осуществлении их деятельности, связанной с выработкой политик, включая деятельность рабочих групп, сформированных организациями поддержки. Конкретные виды деятельности, связанные с

обеспечением безопасности, стабильности и отказоустойчивости, перечислены ниже.

- ***Сотрудники отдела глобальных партнерств*** — отвечают за глобальное и региональное взаимодействие с субъектами ICANN для 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 объем работ, выполняемых отделом глобальных партнерств для корпорации.
- ***Сотрудники отдела связи корпорации*** — отвечают за эффективное доведение информации о планах и программах ICANN и представление организации и ее деятельности сообществу ICANN. Деятельность ICANN, связанная с обеспечением безопасности, стабильности и отказоустойчивости, интегрирована в общую программу связи корпорации.
- ***Сотрудники отдела безопасности*** — отвечают за каждодневное планирование и проведение оперативных мероприятий ICANN, связанных с безопасностью, под руководством Правления и генерального директора ICANN, направленных на выполнение стратегических и оперативных планов корпорации. Эта группа координирует усилия различных подразделений ICANN для обеспечения 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 выявление и доведение до сведения 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 описанного ниже мандата, а также сотрудничает с прочими организациями ICANN, например Организацией поддержки родовых имен (ОПРИ).
- ***Консультативный комитет системы корневых серверов (ККСКС)*** — ККСКС является консультативным комитетом ICANN по вопросам эксплуатационных требований к корневым серверам имен, а также

выполняет анализ и представляет рекомендации по вопросам безопасности системы корневых серверов имен и общей производительности, устойчивости и надежности системы.

В более широком смысле, деятельность, связанная с безопасностью, стабильностью и отказоустойчивостью, осуществляется во всех организациях поддержки и других консультативных комитетах ICANN, как описано ниже.

Сотрудники отдела безопасности ICANN несут общую ответственность за эффективную координацию деятельности корпорации и реализацию интегрированного процесса планирования и отслеживания указанных видов деятельности, а также за обеспечение синхронизации и интеграции работы различных отделов и заинтересованных сторон. На рис. 1 отражены основные организационные взаимоотношения в рамках структуры ICANN.

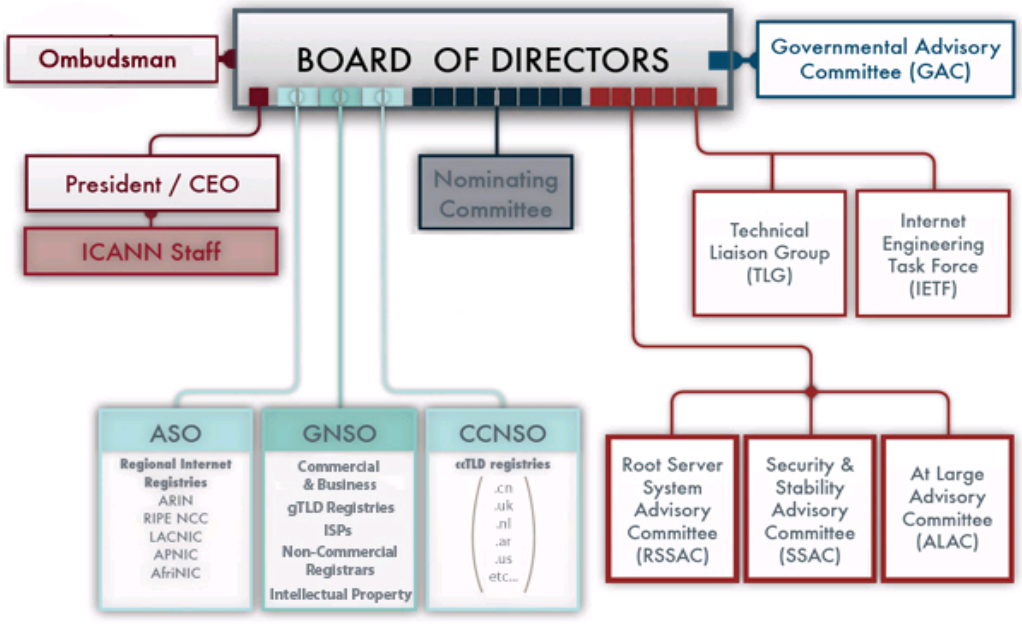


Рис. 1 — организационная структура ICANN

5. Текущие программы ICANN, связанные с безопасностью, стабильностью и отказоустойчивостью

В данном разделе описываются крупные программы и мероприятия, проведенные ICANN и способствующие безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета, с указанием ключевых оперативных партнеров и предпосылок текущих усилий. Целью данного раздела плана является обеспечение базового понимания широкого ряда мероприятий 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, начиная с ключевых функций DNS и адресации, работы с сообществами реестров ДВУ и регистраторов, взаимодействия с региональными интернет-реестрами (РИР) через ОПА, программ корпоративной безопасности и непрерывности работы, деятельности организаций поддержки и консультативных комитетов, равно как и участия в обеспечении глобальной и региональной безопасности, стабильности и отказоустойчивости Интернета.

5.1 Безопасность, стабильность и отказоустойчивость ключевых функций DNS и адресации

5.1.1 Деятельность IANA

ICANN руководит функциями IANA в сотрудничестве с Министерством торговли США, корпорацией 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. Путем

выполнения функций IANA ICANN осуществляет координацию и управление реестрами ключевых идентификаторов, обеспечивая существование глобального, функционально совместимого Интернета.

Хотя Интернет знаменит тем, что является всемирной сетью, свободной от централизованной координации, деятельность ключевых систем уникальных идентификаторов должна координироваться в мировом масштабе — 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 корневой зоной, доменами .int и .arpa, а также ресурсом технологии интернационализированных доменных имен (ИДИ). Методики управления обеспечивают оценку влияния каждого изменения в этих зонах 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 путем развертывания и поддержания отметок о доверии в корневой зоне систем DNS и адресации, способных значительно укрепить целостность данных уникальных идентификаторов, а также целостность откликов в рамках системы DNS.
- ***Адреса и номера автономной системы (АС)*** — IANA осуществляет администрирование и управление глобальным пулом IP-адресов (IPv4 и IPv6) и номеров автономной системы. IANA выделяет эти номерные ресурсы РИР в соответствии с политиками в отношении глобальных номерных ресурсов, которые разрабатываются сообществами РИР в рамках соответствующих процессов разработки политики и координируются в мировом масштабе ОПА. Этот совместный процесс формирования политик позволяет конечным получателям ресурсов добиться консенсуса в мировом масштабе относительно справедливости, предсказуемости и стабильности действий IANA. *ICANN совместно с РИР (через ОПА) и IETF разрабатывает технологию инфраструктуры открытых ключей ресурсов (ИОКР) для введения сертификации номерных ресурсов.*

- ***Назначение протоколов*** — через функции IANA ICANN совместно с IETF осуществляет управление реестрами протоколов и параметров Интернета. ICANN применяет и поддерживает более 700 реестров протоколов и параметров в соответствии со стандартами, разработанными в ходе устоявшегося процесса согласования, заключающегося в публикации запросов комментариев (RFC). В тесном сотрудничестве с IETF и авторами RFC 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 RFC 2860 и в соглашении об уровне обслуживания.

Персонал, ответственный за функции IANA, сотрудничал с сообществом ДВУ при отслеживании внедрения в систему ДВУ общих средств, направленных на смягчение обнаруженной летом 2008 г. уязвимости к «отравлению» кэша DNS (см. доклад «Уязвимость кэша DNS к отравлению, 2008 г.» по адресу http://www.iana.org/about/ presentations/davies-cairo-vulnerability-081103.pdf). ICANN приложит все усилия для того, чтобы ее программы и деятельность укрепляли безопасность, стабильность и отказоустойчивость процессов внесения изменений и дополнений в корневую зону и работу отметок о доверии при запросах в рамках DNS, как описано ниже.

В соответствии с договором о функциях IANA, заключенным ICANN с Министерством торговли, и в рамках ее собственного корпоративного планирования безопасности и реагирования на чрезвычайные происшествия ICANN ежегодно предоставляет Министерству торговли США план обеспечения информационной безопасности, связанный с осуществлением функций IANA. *В январе 2010 г. ICANN успешно провела учения по непрерывности деятельности IANA, см. отчет о результатах выполнения задачи по адресу http://www.icann.org/en/security/iana-business-continuity-exercise-aar-23feb10-en.pdf.*

Ожидается, что ICANN осуществит последнее распределение пространства одноадресной передачи IPv4 между региональными интернет-реестрами (РИР) в течение 2011 календарного года. Это распределение будет осуществляться в соответствии с глобальной политикой

по распределению оставшихся адресов IPv4[2], которая была разработана сообществами РИР и ратифицирована Правлением ICANN в марте 2009 г.

Хотя указанное распределение опустошит пул адресного пространства, находящегося под управлением отдела IANA корпорации ICANN, у РИР все еще останутся пулы адресов, из которых они смогут выделять и назначать адреса поставщикам услуг Интернета и другим операторам сети. РИР продолжают работу над выработкой политик, которые обеспечат доступ новых участников рынка к небольшим блокам адресного пространства IPv4[3] в период между распределением последних пяти блоков «/8s» и внедрением протокола IPv6 большинством сетей, подключенных к Интернету.

РИР также сформулировали политики, позволяющие передавать адресное пространство IPv4 от одного оператора сети к другому[4]. Эти политики разработаны с целью предоставления сетям возможности перемещения адресов туда, где они представляют наибольшую ценность, позволяя продолжить рост сети.

Комитет Правления ICANN по рискам работает над оценкой рисков, с которыми может столкнуться ICANN вследствие сокращения доступного пространства адресов IPv4.

Долгосрочным решением является широкое внедрение протокола IPv6. Хотя был достигнут существенный прогресс, и ряд поставщиков услуг Интернета, таких как XS4all в Нидерландах, начинает предлагать всем своим клиентам IPv6 в качестве стандартной услуги, предстоит проделать еще много работы. На своих конференциях ICANN провела ряд семинаров, направленных на повышение осведомленности об указанной проблеме, в то время как

[2] http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm

[3] http://www.nro.net/documents/comp-pol-201006.html#2-6

[4] http://www.nro.net/documents/comp-pol-201006.html#1-3-2

РИР реализуют обучающие программы по вопросам IPv6 и по повышению осведомленности[5][6][7][8][9].

Важным моментом, о котором не следует забывать, является то, что существующий Интернет продолжит свою работу даже после распределения региональными интернет-реестрами всех своих резервов IPv4. В течение определенного периода некоторые сети будут доступны по протоколу IPv6, а некоторые нет. Однако IPv6 позволит операторам продолжить расширение своих сетей за рамки ограничений, налагаемых протоколом IPv4.

5.1.2 Операции DNS

ICANN выступала в защиту необходимости внедрения DNSSEC на корневом уровне. *Со времени введения первоначального плана по БСО корпорация ICANN, VeriSign и NTIA добились существенного прогресса в реализации DNSSEC через масштабное внедрение, которое привело к общему подписанию корневой зоны в июле 2010 г. Первая церемония генерации ключа подписи ключа (KSK) для DNSSEC была проведена в Кульпереpе, Вирджиния, 16 июня 2010 года (см. http://www.icann.org/en/announcements/announcement-4-16jun10-en.htm), а вторая церемония генерации KSK была проведена 12 июля 2010 г. в Лос-Анджелесе, Калифорния, для обеспечения подписания корневой зоны. Развертывание DNSSEC в корневой зоне выгодно субъектам, публикующим информацию в DNS, позволяет интернет-сообществу и конечным пользователям размещать в корневой зоне данные криптографических ключей (отметки о доверии) и защитить распознаватели DNS от «отравления» кеша.*

ICANN начала подписывать .arpa многие другие домены, принадлежащие корпорации. Подготовительная работа включает ведущееся с июня 2007 г. внедрение тестовой платформы для DNSSEC, сотрудничество с ДВУ и прочими операторами DNS относительно усилий по внедрению

[5] http://www.afrinic.net/training/ipv6training.htm

[6] http://www.apnic.net/services/services-apnic-provides/training/courses/ipv6-essentials

[7] https://www.arin.net/knowledge/v4-v6.html

[8] http://lacnic.net/en/eventos/ipv6/

[9] http://www.ripe.net/training/ipv6/outline.html

DNSSEC, приобретение технических навыков использования 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 безопасного внедрения DNSSEC, включая подписание icann.org и iana.org. Наконец, для обеспечения дальнейшего продвижения DNSSEC ICANN организовала репозиторий отметок о доверии IANA для доменов верхнего уровня (РОД-I) как способ обеспечить доступность ключей DNSSEC для ДВУ, уже внедривших эту технологию, для тех, кто внедряет DNSSEC в настоящее время.

ICANN сотрудничает с операторами корневых серверов имен в сфере безопасной и стабильной координации корневой зоны в обеспечение адекватного планирования на случай чрезвычайных происшествий и для поддержания четкости процессов при внесении изменений в корневую зону. ICANN продолжит сотрудничество с операторами корневых серверов имен и прочими субъектами в сфере безопасной и стабильной координации системы корневых серверов. ККСКС выступал в роли ключевого консультанта по вопросам воздействия на систему изменений в протоколах, таких как добавление в корневую зону записей IPv6.

Кроме того, ICANN отвечает за работу корневого сервера имен *l.root-servers.net.* В рамках этой роли оператора сотрудники ICANN также взаимодействуют на оперативном уровне с операторами прочих корневых серверов. Как оператор корневого сервера «L» ICANN также принимает активное участие в деятельности сообщества DNS, включая вклад в такие инициативы сообщества, как Операционный, аналитический и исследовательский центр системы доменных имен (DNS-OAИЦ) и исследовательский проект «Один день из жизни Интернета» Кооперативной ассоциации по анализу данных Интернета (КААДИ). ICANN стремится к использованию своей деятельности для поддержки многообразия и понимания передового опыта, а также стремится приобретать и передавать знания. *Оперативная группа DNS также поддерживала исследование масштабирования корневой зоны «L», http://www.icann.org/en/announcements/announcement-17sep09-en.htm.*

В 2009 г. ICANN повысила отказоустойчивость корневого сервера «L», создав экземпляры в Праге, Чешская Республика, и Стамбуле, Турция. Дополнительные усовершенствования запланированы на 2010 и 2011 ФГ.

5.2 Безопасность, стабильность и отказоустойчивость реестров ДВУ и регистраторов

Фундаментальной и непосредственной обязанностью ICANN, связанной с безопасностью, стабильностью и отказоустойчивостью Интернета, является управление соглашениями с реестрами рДВУ и аккредитованными ICANN регистраторами, и разработка базовой структуры соглашений, используемых для управления взаимоотношениями с реестрами рДВУ. ICANN заключила договоры с 16 реестрами рДВУ и более чем 900 аккредитованными регистраторами, несущими ответственность за координацию регистрации доменных имен и обеспечение их разрешения в DNS. Обязанности этих сторон, с которыми заключены договоры, очерчены в соглашениях о реестре (СР) 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 путем включения положений, улучшающих стабильность и отказоустойчивость, как описано ниже.

5.2.1 Реестры рДВУ

ICANN сотрудничает с операторами рДВУ в части координации безопасной и стабильной работы этих ДВУ. Все реестры рДВУ поддерживают договорные отношения с ICANN. При том, что некоторые элементы этих договоров 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 имен (ОПРИ) и принятые ICANN. Прочие положения соглашений, способствующие безопасной и стабильной работе реестров, включают требование передачи информации на ответственное хранение третьим сторонам, а также соглашения об уровне обслуживания для услуг DNS, совместной регистрационной системы и операций серверов имен. В договорах между ICANN и рДВУ указываются требования к доступности, эксплуатационным показателям и центрам обработки данных. В 2007 г. ICANN стала инициатором усилий по планированию непрерывности

работы реестров рДВУ, результатом которых стало создание рабочего плана, а также принятие обязательств по проведению ряда ежегодных плановых учений с целью повышения способности сообщества реестров рДВУ справляться с проблемами и отказами системы реестров и регистраторов.

В 2006 г. ICANN ввела процесс оценки услуг реестров (ПОУР) в качестве средства содействия своевременному и предсказуемому механизма ввода новых услуг реестров. Ключевым компонентом ПОУР является определение потенциальной возможности предложенной услуги создавать угрозу безопасности или стабильности. Если выясняется, что предлагаемая услуга способна представлять угрозу безопасности или стабильности, предложение передается на рассмотрение комиссии технических экспертов, названной группой технической оценки услуг реестра (ГТОУР). ГТОУР производит анализ предлагаемой услуги и представляет Правлению ICANN рекомендацию одобрить или отклонить услугу.

В октябре 2009 г. был введен процесс ускоренного рассмотрения запросов о безопасности реестра (УЗБР) (см. http://www.icann.org/en/registries/ersr/). УЗБР был разработан для предоставления реестрам рДВУ процедуры информирования ICANN о текущем или неизбежном нарушении безопасности в соответствующем ДВУ или DNS и запроса о временном освобождении от ответственности по договору за действия, которые они могут предпринять или уже предприняли, чтобы сократить или устранить последствия происшествия. Освобождение от ответственности по договору — это освобождение от выполнения требований конкретного положения соглашения о реестре на период, необходимый для реагирования на происшествие. УЗБР предназначен для сохранения безопасной работы в период происшествия с одновременным надлежащим информированием соответствующих сторон (например, ICANN, других заинтересованных поставщиков и т.п.).

5.2.2 Новые рДВУ и ИДИ

В течение 2010 ФГ и в 2011 ФГ ICANN вместе с сообществом продолжает работу над усовершенствованием подходов к сокращению возможностей для злонамеренного поведения в новых рДВУ [см. пояснительную записку по сокращению возможностей для злонамеренного поведения от 28 мая

2010 г., http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf].

Запустив процедуру ускоренного ввода нДВУ с ИДИ в ноябре 2009 года и осуществляя подготовку к включению ИДИ в программу новых рДВУ, ICANN признает необходимость усилий по обеспечению безопасной, стабильной и отказоустойчивой работы новых компонентов DNS и всей системы в целом. Процесс подачи и анализа заявок на новые рДВУ включает техническую оценку способности кандидата управлять реестром, а также соответствия строк техническим требованиям, сформулированным в RFC, согласно протоколу интернационализации доменных имен в приложениях (ИДИП) и руководству по ИДИ.

ICANN запустила процедуру ускоренного ввода нДВУ с ИДИ 16 ноября 2009 г. (см. http://www.icann.org/en/topics/idn/fast-track/). Со времени запуска программы было получено 34 запроса на 22 различных языках (см. http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm). Эти строки в настоящее время проходят этап делегирования IANA, и первые строки нДВУ с ИДИ были введены в корневую зону в мае 2010 г. для Египта, Саудовской Аравии, Объединенных Арабских Эмиратов и Российской Федерации. Правление ICANN одобрило делегирование строк Китаю, Гонконгу и Тайваню на конференции ICANN в Брюсселе, состоявшейся в июне 2010 г., а строки для Шри-Ланки, Тайланда, Оккупированной палестинской территории, Иордании и Туниса были одобрены в августе 2010 г.

Первоначальный ввод нДВУ с ИДИ в рамках процесса ускоренного ввода ограничен неконфликтными строками, отражающими наименования стран и территорий, соответствующих существующим нДВУ.

В рамках процесса ускоренного ввода независимая группа экспертов, Комиссия по стабильности DNS, проводит оценку предлагаемой строки нДВУ с ИДИ на похожесть и отсутствие потенциальных конфликтов с требованиями безопасности и стабильности для строк ИДИ. Ожидается, что в рамках процесса ввода новых рДВУ будет создана аналогичная комиссия экспертов для проведения технической оценки кандидатов и предлагаемых ими ДВУ. Механизм внедрения новых рДВУ дополнительно предполагает предварительную реализацию процесса оценки услуг реестра (ПОУР) для оценки потенциальных проблем в сфере безопасности и стабильности новых услуг реестров, предлагаемых в заявке на рДВУ.

Кроме того, перед делегированием домена все кандидаты должны будут пройти техническую проверку на соответствие техническим требованиям к эксплуатации реестра.

ICANN намеревается проанализировать процесс реализации процедуры ускоренного ввода нДВУ с ИДИ в 2011 ФГ.

5.2.3 Регистраторы рДВУ

ICANN сотрудничает с регистраторами по вопросам безопасности, стабильности и отказоустойчивости. 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 имен, помимо прочих, которые различными способами содействуют безопасности, стабильности и отказоустойчивости DNS. *В 2009 г. было введено улучшенное CAP, и в настоящее время свыше 95% регистраций рДВУ охвачено CAP 2009 через добровольное подписание этого соглашения регистраторами. В ответ на запрос Расширенного консультативного комитета ICANN также опубликовала Руководство по CAP 2009 для лиц, не имеющих юридической подготовки (http://www.icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm).*

Сотрудники отдела по связям с регистраторами ICANN играют роль первой линии связи при повседневном отслеживании соответствия регистраторов требованиям CAP путем неформального разрешения жалоб владельцев регистрации и разногласий между регистраторами, а также путем периодического анализа аккредитации (например, после обновления CAP регистратора).

В поддержку более стабильной системы доменных имен ICANN разработала программы и процедуры на случай неспособности регистратора выполнять свои обязательства. 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 аккредитации,

регистратору, аккредитованному ICANN. Кроме того, сотрудники ICANN используют ряд внутренних оперативных механизмов, направленных на поддержание здоровой среды регистрации доменов и предотвращение нарушений в работе владельцев регистрации и пользователей Интернета в случае неспособности регистратора выполнять свои обязательства.

5.2.4 Служба WHOIS

Службы WHOIS предоставляют общий доступ к информации по зарегистрированным доменным именам, которая в настоящий момент включает в себя контактные данные держателей зарегистрированных имен. ICANN играет определенную роль в администрировании разработанных сообществом правил для системы WHOIS в рамках рДВУ. Объем данных, собираемых при регистрации доменного имени, и способы доступа 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 серверов имен и регистраторов, даты создания доменов и сроки истечения регистрации, контактную информацию зарегистрированного держателя имени, реквизиты для связи по техническим и административным вопросам и предоставлять к ним бесплатный открытый доступ.

WHOIS применяется различными сообществами для ряда целей, включая содействие технической координации и предоставлению информации об организациях и лицах, подозреваемых в возможных злоупотреблениях DNS. Деятельность ICANN сосредоточена на обеспечении выполнениями реестрами рДВУ и аккредитованными ICANN регистраторами своих 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 признает обоснованность озабоченности вопросами конфиденциальности и безопасности, выражаемой различными лицами по поводу предоставления информации о них посредством WHOIS. ICANN не прекращает усилий по устранению этой озабоченности. Признавая, что с течением времени надежность и полезность существующей службы WHOIS может

снизиться, а также по указанию ОПРИ, персонал ICANN сформулировал всеобъемлющий набор требований к WHOIS, включающий известные недостатки обслуживания в настоящее время и возможные требования, необходимые для поддержки будущих инициатив в области политики. [справочные документы: Организация поддержки родовых имен ICANN (ОПРИ), резолюции Совета, май 2009 г. Марина дель Рей, Калифорния: ICANN. Выборка от 25 октября 2009 г. из http://gnso.icann.org/resolutions/#200905]. В этом отчете предпринята попытка определить технические требования, которые могут оказаться необходимыми для исправления недостатков и реализации будущей политики в отношении WHOIS. Ряд элементов этого списка заимствован из рекомендаций ККБС для ОПРИ, демонстрирующих приверженность ICANN, через совместное рассмотрение ОП и КК мер по усовершенствованию WHOIS, к поиску решений, сохраняющих полезность WHOIS с одновременным учетом аспектов конфиденциальности и безопасности информации WHOIS.

5.2.5 Выполнение договорных обязательств

Отдел выполнения договорных обязательств обеспечивает выполнение со стороны ICANN и ее партнеров по договорам требований, установленных в соглашениях между сторонами. В его задачи входит управление системой ICANN по приему претензий, позволяющей общественности регистрировать жалобы, связанные с доменными именами, которые могут относиться к вопросам безопасности, стабильности или отказоустойчивости. См. веб-сайт по адресу http://reports.internic.net/cgi/registrars/problem-report.cgi. Персонал отдела выполнения договорных обязательств расследует претензии, относящиеся к возможному нарушению CAP, и в случае обнаружения нарушения предпринимает меры по обеспечению выполнения обязательств. Хотя 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.

Отдел выполнения договорных обязательств также управляет системой отчетов о проблемах данных WHOIS (WDPRS), доступ к которой можно получить по адресу http://wdprs.internic.net/. WDPRS 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. По согласованию с сообществом система WDPRS была изменена в 2008 г. с учетом вызывающих озабоченность вопросов функциональности, ограниченных возможностей и недостаточного соблюдения требований. Видоизмененная система WDPRS была запущена в декабре 2008 г. Отдел выполнения договорных обязательств продолжает дорабатывать эту систему с целью повышения точности данных WHOIS.

ICANN уполномочила Национальный центр исследования общественного мнения Университета Чикаго на проведение исследования точности данных WHOIS. Предварительный отчет был опубликован 15 февраля 2010 г., http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm.

5.2.6 Защита владельцев регистрации рДВУ

ICANN также стремится различными способами обеспечивать уверенность владельцев регистраций в безопасности, стабильности и отказоустойчивости DNS. Защита в этих областях предоставляется посредством положений в договорах, соглашениях и программах ICANN по обеспечению выполнения договорных обязательств. ICANN предоставляет владельцам регистрации информацию об обязательствах регистраторов в рамках CAP и средствах подачи претензий через веб-сайт InterNIC по адресу http://www.internic.net/. ICANN также ведет разъяснительную деятельность в сообществе регистраторов, поощряя поддержку IPv6 для лиц, регистрирующих домены.

Помимо этого, работа организаций поддержки и консультативных комитетов ICANN сосредоточена на решении вопросов, касающихся безопасности, стабильности и отказоустойчивости, вызывающих озабоченность владельцев регистраций. В последних рекомендациях ККБС сформулированы практические методы, возможность использования которых должны рассматривать регистраторы для защиты доменных имен и учетных записей регистрации доменов от несанкционированного доступа и для защиты сведений о конфигурации DNS от неправомерного использования.[10] *Проекты ККБС на 2010 г. включают подготовку дополнительного отчета, в котором будут сформулированы практические методы, которые владельцы регистраций смогут использовать самостоятельно для упреждающего контроля и защиты учетных записей регистрации доменов и сведений о конфигурации DNS от неправомерного использования. Прочая деятельность ККБС включает подготовку документов относительно запрета использования переадресации доменами верхнего уровня [SAC041], развертывания DNSSEC, официального списка контактных лиц для борьбы со злоупотреблениями [SAC038] и обработки потерянных записей DNS.*

Ряд вопросов, касающихся защиты владельцев регистраций, был поднят Расширенным консультативным комитетом (РКК). Сначала РКК поднял вопрос о пробном использовании

[10] См. SAC 40, Меры по защите услуг регистрации доменов от неправомочного или недопустимого использования, 19 августа 2009 г. (http://www.icann.org/en/committees/security/sac040.pdf).

доменов, что привело к принятию Советом ОПРИ и Правлением новой согласованной политики, направленной на предотвращение злоупотреблений периодом пробного использования доменов. *Недавно РКК рассмотрел озабоченность Совета ОПРИ вопросами восстановления владельцами регистрации доменных имен после истечения срока их действия (ВДИСД), а также прозрачности и подотчетности регистрации доменных имен [http://www.atlarge.icann.org/announcements/announcement-19jul10-en.htm].* ОПРИ также выступает с рядом дополнительных инициатив, обладающих потенциалом укрепления защиты владельцев регистраций, таких как улучшения политики изменения регистраторов, включая соображения по необходимости электронной аутентификации, и доработка политики в отношении 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 программе внедрения системы подотчетности, 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 развитию мощностей для планирования реагирования на нападения и чрезвычайные происшествия. Персонал ICANN тесно сотрудничает с операторами ДВУ, информируя последних о проблемах безопасности через функции IANA, программу планирования реагирования на нападения и чрезвычайные происшествия (ПРНЧП) и усилия региональных представителей отдела глобальных партнерств. IANA развила доверительные взаимоотношения с операторами ДВУ благодаря улучшению своих рабочих показателей и разъяснительной работе в сообществе операторов ДВУ, что способствует осуществлению совместного реагирования в требующих глобальной координации ситуациях, связанных с DNS.

5.2.8 Технические требования IANA

Через управление функциями IANA корпорация ICANN также помогает обеспечить соответствие ДВУ техническим требованиям в поддержку стабильной и безопасной работы. Конкретные требования к серверам имен обеспечивают доступность доменов в DNS, а персонал, ответственный за функции IANA, тесно сотрудничает с менеджерами ДВУ при решении проблем, возникающих при соблюдении этих технических стандартов. ICANN не вмешивается в эксплуатацию нДВУ, но готова оказывать содействие в ситуациях, когда необходимо быстро и надежно вносить изменения в соответствующие данные корневой зоны. Основная цель ICANN — обеспечить стабильность и безопасность зоны ДВУ и корневой зоны.

5.2.9 Совместное реагирование на злоупотребления системой доменных имен

ICANN сотрудничает с рядом организаций, стремясь обеспечить заинтересованным сторонам возможность анализировать деятельность, которая может представлять собой злоупотребление DNS. С конца 2008 г. значительно активизировалось распространение зловредных программ, использующих ресурсы DNS. Одним из таких происшествий, заслуживающим упоминания, является червь Conficker [сводная информация о Conficker и анализ, http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf]. Вместе с сообществами, занимающимися вопросами безопасности, операторами реестров ДВУ и сообществами правоохранительных органов ICANN принимала участие в глобальном совместном реагировании с целью сдержать распространение червя Conficker. ICANN опубликовала отчет под названием «Сводная информация о Conficker и анализ», в котором была документально зафиксирована хронология событий, относящихся к сдерживанию распространения Conficker, обсуждались извлеченные уроки и предлагались пути улучшения будущих совместных усилий (например, разработанный ICANN процесс УЗБР). ICANN продолжает работу с реестрами и регистраторами, направленную на обеспечение осведомленности и содействие распространению информации об относящихся к DNS происшествиях глобального масштаба в сфере безопасности. Мандат ICANN в этой области ограничен, и поэтому корпорация на равных правах принимает участие в обсуждениях путей обеспечения эффективного

реагирования на возникновение конкретных рабочих ситуаций.

Для содействия расширению сотрудничества в этой области персонал ICANN поддерживает усилия ОПНИ по реагированию на происшествия в зоне нДВУ. В феврале 2010 г., ICANN опубликовала Экономическое обоснование глобальной концепции DNS-CERT (http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf) для интернет-сообщества. Это экономическое обоснование содержит описание требований и возможных расходов с учетом варианта использования указанной функции DNS-CERT другими членами сообщества. Со времени опубликования экономического обоснования DNS-CERT, обсуждения комментариев общественности (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf) и дискуссий на конференциях ICANN в Найроби и Брюсселе, ICANN работает с заинтересованными субъектами над определением подходов к системе совместного реагирования на нарушения безопасности DNS, не находящейся под управлением ICANN, но разрабатываемой в сотрудничестве с сообществом.

5.2.10 Обеспечение общей безопасности и отказоустойчивости DNS

Хотя ни один из отдельных субъектов не несет 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 осуществляет анализ и предоставляет свои рекомендации сообществу DNS. Рекомендация SSAC 004, *Защита границ*, содержит фундаментальный анализ проблем в сфере безопасности систем уникальных идентификаторов.[11] Среди ключевых усилий можно привести анализ и рекомендации, связанные с атаками типа «отказ в обслуживании» (DDoS), внедрением DNSSEC с добавлением записей IPv6 в корневую зону DNS, опережающим использованием доменных имен, хостингом «Fast Flux» и захватом доменных имен. Кроме того, члены ККБС принимают участие в деятельности Комитета по вопросам политики Интернета, сформированного в рамках рабочей группы по борьбе с фишингом (РГБФ), и являются соавторами технических документов с описанием способов

[11] SAC 004, Защита границ, 17 октября 2002 г., http://www.icann.org/en/committees/security/sac004.pdf.

использования фишерами имен субдоменов и методов, которые организации могут использовать при реагировании на нападения на веб-сайты, а также сотрудничают с Группой интеллектуальной собственности (IPC) при изучении наиболее широко используемых уязвимостей веб-сайтов.

ICANN планирует и в дальнейшем развивать эту роль, стремясь к выявлению возможностей 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, сложностям обеспечения безопасных, стабильных и отказоустойчивых операций DNS в средах с ограниченными ресурсами и борьбе с неправомерным использованием DNS в противозаконных целях. Этот отчет доступен по адресу http://www.gtisc.gatech.edu/icann09. *Второй симпозиум по безопасности, стабильности и отказоустойчивости DNS был проведен в Киото, Япония, в феврале 2010 г., см. http://dns-srr.e-side.co.jp/, а отчет был опубликован в апреле 2010 г. по адресу http://www.icann.org/en/announcements/announcement-26apr10-en.htm.*

Кроме того, сотрудники ICANN, организации поддержки и консультативные комитеты ICANN начали повышать интенсивность сотрудничества в рамках проектов с участием множества заинтересованных сторон с целью улучшения способности корпорации осуществлять эффективное формулирование политики, обеспечивать выполнение договорных обязательств и по ряду других инициатив, связанных с решением проблем в области безопасности и отказоустойчивости, стоящих перед DNS и присущих этой системе.

5.2.11 Достоверность, право использования и уникальность номерных ресурсов Интернета

Через управление функциями IANA корпорация ICANN обладает стратегическими возможностями и несет ответственность за стабильность, безопасность и

отказоустойчивость системы распределения номеров Интернета и, в конечном итоге, через инфраструктуру открытых ключей ресурсов (ИОКР), за глобальную систему маршрутизации Интернета. Эта ответственность подразумевает необходимость внедрения идеального в техническом отношении приложения в виде единой отметки о доверии ИОКР, как было указано Советом по архитектуре интернета (IAB)[12] и Организацией номерных ресурсов (ОНР)[13], и приводит в результате к возможности полной сертификации достоверности, прав использования и уникальности номерных ресурсов Интернета. ICANN ее персонал предприняли существенные усилия по совместной работе с IETF и другими специальными рабочими группами, принимая участие в стандартных процессах, обменивась информацией с заинтересованными сторонами и развертывая пробную реализацию инфраструктуры ИОКР (в настоящее время выведенную из эксплуатации).

ICANN стремится к взаимодействию со всеми субъектами ИОКР, а сотрудники корпорации инициировали процессы таким образом, чтобы обеспечить развертывание наиболее целесообразного технического решения и его доступность для интернет-сообщества в соответствующие сроки и с учетом необходимости в обсуждении.

5.3 Глобальная разъяснительная работа в сфере безопасности (привлечение к работе, осведомленность)

5.3.1 Глобальные партнеры и программы

В основе глобальной стратегии ICANN по участию в работе по обеспечению безопасности, стабильности и отказоустойчивости лежит эффективное партнерство с рядом организаций. Многие из этих усилий осуществляются под руководством сотрудников Отдела глобальных партнерств ICANN. ICANN принимает активное участие в широком спектре международных форумов, связанных с Интернетом, включая несколько, посвященных вопросам безопасности, стабильности и отказоустойчивости Интернета. Приведенный ниже перечень партнеров и проектов не является исчерпывающим, и ICANN будет стремиться привлекать к

[12] http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html

[13] http://www.nro.net/news/nro-declaration-rpki.html

работе других по мере возникновения возможностей. Корпорация имеет следующих ключевых глобальных партнеров.

- ***Комиссия по технологиям Интернета (IETF) и Совет по архитектуре Интернета (IAB)*** — возглавляют усилия по определению технологических подходов к повышению безопасности Интернета, сосредоточенные на разработке более мощных протоколов и рабочих практических методов. ICANN работает вместе с IETF над созданием протоколов, связанных с назначением имен и адресов, и стремится обеспечивать их развертывание в ядре Интернета, способствуя обеспечению безопасности общей среды. В частности, ICANN будет принимать участие в усилиях по созданию протоколов, обеспечивающих более безопасную основу Интернета, и сосредоточенных на таких проектах как DNSSEC и ИОКР.
- ***Общество Интернета (ISOC)*** — стимулирует осведомленность 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 совместно с ISOC работает над обеспечением осведомленности и расширением возможностей поддержания безопасности, стабильности и отказоустойчивости. ICANN планирует продолжать сотрудничество в рамках продолжающейся совместной программы ISOC и ICANN по обучению операторов ДВУ, включая обучение техническим аспектам повышения безопасности и смягчению последствий кибератак и нарушений в работе.
- ***Форум управления Интернетом (IGF)*** — форум IGF поддерживает диалоги по кибербезопасности и доверию между различными заинтересованными сторонами. Кроме того, IGF выработал подход к управлению критически важными ресурсами Интернета и борьбе с киберпреступлениями. ICANN будет по-прежнему принимать участие в работе IGF, включая распространение информации о своей собственной роли в обеспечении безопасности, стабильности и отказоустойчивости системы уникальных идентификаторов Интернета, а также вносить свой вклад в глобальный диалог, ведущийся на этом форуме.

- ***Операционный, аналитический и исследовательский центр DNS (DNS-OARC)*** — ICANN останется спонсором и активным участником всего спектра проектов DNS-OARC.

5.3.2 Региональные партнеры и программы

ICANN установила региональные связи с разнообразными партнерами и в рамках разнообразных мероприятий. Ключевые аспекты региональной деятельности ICANN представлены ниже.

- ***Региональные ассоциации нДВУ*** — помимо сотрудничества по программе ПРНЧП, описанного ниже, ICANN продолжит оказывать содействие и передавать экспертные знания в рамках мероприятий, спонсируемых этими организациями.
- ***Региональные сетевые информационные центры (РСИЦ) и группы операторовсетей (ГОС)*** — ICANN по-прежнему будет участвовать в этих форумах в обеспечение того, чтобы деятельность корпорации наилучшим образом позволяла 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 рамках усилий по поддержке наращивания потенциала DNS в сотрудничестве с Азиатско-Тихоокеанской ассоциацией ДВУ (APTLD) и продолжает пользоваться мощной поддержкой для осуществления деятельности в указанном регионе. ICANN продолжит свое участие в региональных форумах, таких как Основы управления Интернет-ресурсами, с целью предоставления оперативных консультаций и обучения, связанных с безопасностью и отказоустойчивостью DNS по мере возникновения возможностей.
- ***Европа*** — ICANN продолжит свое участие 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) при проведении 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 в целях расширения международного диалога по кибербезопасности. В частности, в 2008 и 2010 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 в 2011 г.

- ***Африка и Латинская Америка*** — совместно с региональными организациями ISOC, а также в рамках прочих соответствующих форумов ICANN продолжит осуществлять проекты, связанные с кибербезопасностью. Совместно с ассоциацией LACTLD в 2009 и 2010 гг. корпорация ICANN предлагала курсы подготовки в области безопасности и отказоустойчивости нДВУ. ICANN также проводит курсы в области нДВУ совместно с ассоциацией африканских доменов верхнего уровня (AfTLD), ISOC-Africa и APTLD в Азии.

5.3.3 Работа с правительствами

ICANN сотрудничает с правительствами по всему миру в стремлении обеспечить безопасность, стабильность и отказоустойчивость систем уникальных идентификаторов Интернета. ICANN по-прежнему будет доводить до остальных свою точку зрения на оперативные и технические 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 структуры ICANN Правительственный консультативный комитет (ПКК) будет получать регулярные отчеты об усилиях корпорации в области безопасности, стабильности и отказоустойчивости и вносить свой вклад в эти программы в рамках процесса стратегического планирования. ICANN продолжит активно определять свою роль в международных обсуждениях вопросов безопасности и их значения для управления безопасностью и отказоустойчивостью систем уникальных идентификаторов. ICANN будет сотрудничать с ООН, международными, межправительственными и региональными организациями, направляя свои усилия на содействие региональным проектам, нацеленным на повышение безопасности и отказоустойчивости DNS. Такие проекты будут основываться на меморандумах о взаимопонимании, заключенных ICANN с рядом организаций.

Например, ICANN продолжит участвовать в форумах по кибербезопасности, таких как постоянные усилия ОЭСР по борьбе со зловредными программами. ICANN также продолжит участвовать в аналогичных проектах АТЭС и других организаций в этой области.

Кроме того, на открытых международных конференциях ICANN ПКК предоставляет корпорации свои руководящие указания в форме коммюнике.

5.4 Взаимодействие с региональными интернет-реестрами

ICANN сотрудничает с ОПА путем взаимодействия с Организацией номерных ресурсов (ОНР). Через это взаимодействие ICANN работает с региональными интернет-реестрами РИР, что позволяет корпорации и РИР поддерживать и повышать безопасность, стабильность и отказоустойчивость Интернета на благо местных и глобальных пользователей. 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 для субдоменов .arpa, включая ip6.arpa и in-addr.arpa. РИР осуществляют разработку средств, позволяющих обеспечить сертификаию IP-адресов и номеров автономной системы (АС) в рамках усилий по созданию инфраструктуры ИОКР. РИР также несут ответственность за назначение номеров автономной системы (НАС), и ICANN следует стремиться к партнерству с РИР в целях обеспечения целостности этих назначений. В ближайшей перспективе эти усилия обеспечат достоверную связь между держателем номерного ресурса и самим номерным ресурсом. Такая иерархическая система сертификации может служить в качестве основы для разработки средств подтверждения маршрутов Протокола пограничного шлюза. ICANN сохранит свое стремление к сотрудничеству в рамках этих усилий.

5.5 Корпоративная безопасность ICANN и операции по обеспечению непрерывности деятельности

ICANN обеспечивает безопасность, стабильность и отказоустойчивость собственных операций при руководстве

IANA и выполнении остальных ключевых функций в рамках системы DNS и системы адресации, а также стремится выполнять свои обязанности в качестве корпорации и участника сообщества, вносящего свой вклад в обеспечение общей безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов Интернета. ICANN обеспечит возможности эффективного реагирования и работы с соответствующими органами власти, если ее собственные активы подвергнутся нападению со стороны злоумышленников.

ICANN взяла на себя обязательство реализации постоянно действующей программы обеспечения безопасности, нацеленной на управление рисками для информации, персонала и физических активов организации. Осенью 2008 г. ICANN назначила директора по безопасности, несущего ответственность за эти программы. ICANN предоставляет информационные активы, услуги и технологию в поддержку IANA и других критически важных операций. Последние усилия были сосредоточены на переоценке, документировании и развертывании более надежных процессов и политик в области безопасности. *На основании плана информационной безопасности ICANN, соответствующего стандартам ISO 27002, постоянно осуществляется улучшение 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 и физических активов ICANN сосредоточено на защите персонала и объектов ICANN, необходимых для ведения глобальной деятельности ICANN, включая обеспечение безопасности во время международных конференций корпорации. ICANN установила процесс планирования для управления рисками, связанными с безопасностью в масштабах всего предприятия и использует собственный отдел внутренней безопасности наряду с поддержкой со стороны консультантов по безопасности.*

Программы безопасности ICANN являются частью общей программы управления корпоративными рисками, реализуемой под наблюдением Правления ICANN, а также взаимно поддерживающих друг друга корпоративных программ обеспечения непрерывности деятельности. ICANN развила свои процессы управления рисками благодаря разработке Руководства по управлению рисками для организации, созданию группы по надзору за управлением

рисками и проведению регулярной оценки важнейших рисков организации, а также отчетности по управлению рисками для важнейших инициатив ICANN.

По мере роста ICANN растет и база активов корпорации наряду с масштабами ее международной деятельности и общественной значимостью. ICANN продолжает уделять особое внимание управлению рисками, непрерывности и безопасности деятельности корпорации как фундаментальным составляющим своего корпоративного механизма.

5.6 Деятельность организаций поддержки и консультативных комитетов ICANN

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. Три организации поддержки ICANN — Организация поддержки родовых имен (ОПРИ), Организация поддержки национальных имен (ОПНИ), и Организация поддержки адресов (ОПА) — отвечают за разработку политики, включая вопросы, имеющие отношение к безопасности и стабильности. Конкретные сведения о каждой организации поддержки и ее процессах можно найти по следующим 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 различных договоров, соглашений, меморандумов о взаимопонимании и действий сотрудников. ОПРИ прежде всего отвечает за политики, связанные с соглашениями реестров и регистраторов рДВУ с учетом всех изменений политики WHOIS рДВУ, анализ вопросов, связанных, среди прочего, с хостингом «Fast Flux», истечением срока действия доменных имен, изменением регистраторов доменных имен и политиками борьбы со злоупотреблениями при регистрации.

В данный момент ICANN работает с сообществом над пересмотром существующего процесса разработки политики (ПРП) рДВУ для повышения его эффективности и восприимчивости к нуждам корпорации в сфере разработки политики. Среди многочисленных изменений, предусмотренных в существующем ПРП, 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 постановке целей сложных задач в сфере формулирования политики, а также на разработку улучшенных способов оценки эффективности новых политик.

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

ОПА координирует разработку политики в отношении осуществляемого IANA распределения IP-адресов и номеров автономной системы между РИР. Разработкой этих глобальных политики занимаются отдельные сообщества РИР. Функции ОПА заключаются в сборе этих регионально разработанных политик и их согласовании с целью объединения в единую глобальную политику, которая затем передается на ратификацию в Правление ICANN.

Кроме того, в состав ICANN входят четыре консультативных комитета, которые предоставляют свои рекомендации Правлению и сообществу корпорации: Расширенный консультативный комитет (РКК), Правительственный консультативный комитет (ПКК), Консультативный комитет системы корневых серверов (ККСКС) и Консультативный комитет по безопасности и стабильности (ККБС). Конкретные сведения относительно функций, процессов и деятельности этих комитетов можно найти по адресу http://www.icann.org/en/committees/. Эти консультативные комитеты часто сотрудничают между собой и с организациями поддержки по различным проектам. В первую очередь это касается ККБС. Сотрудники отдела политик ICANN оказывают комитетам поддержку при проведении исследований, анализе и подготовке рекомендаций.

ККБС консультирует сообщество и Правление ICANN по вопросам, связанным с безопасностью и стабильностью систем распределения имен и адресов Интернета. К таким вопросам относятся правильное и надежное функционирование корневой системы имен, распределение адресов и назначение номеров Интернета, а также услуги реестров и регистраторов рДВУ, такие как WHOIS. ККБС занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и адресов Интернета с целью определения источников основных угроз стабильности и безопасности, и предоставляет соответствующие рекомендации сообществу ICANN. Подробные сведения о

деятельности ККБС можно найти по адресу www.icann.org/en/committees/security.

Помимо упомянутого выше, прочая текущая деятельность организаций поддержки и консультативных комитетов включает совместные обсуждения вопросов, связанных с безопасностью и стабильностью и представляющих обоюдный интерес в рамках групп на конференциях ICANN, организацию семинаров и брифингов по вопросам, связанным с безопасностью и стабильностью, а также оповещение сообщества о деятельности, связанной с политикой, посредством ежемесячного отчета о политике (http://www.icann.org/en/topics/policy/).

Соответствующая работа по формированию политики ОПРИ включает следующее:

Fast Flux

Процесс разработки политики (ПРП) ОПРИ в отношении хостинга Fast Flux был завершен в сентябре 2009 г. В отчете РГ были выявлены лица, получающие выгоду от использования «Fast Flux», и лица, которым причиняется вред, описано влияние хостинга «Fast Flux» на пользователей Интернета, а также сделаны выводы в отношении того, приведут ли технические изменения и пересмотр политики DNS к снижению отрицательного влияния хостинга «Fast Flux». В сентябре 2009 г. Совет ОПРИ принял предложение создать проектную группу для разработки рабочего плана внедрения рекомендаций, предложенных рабочей группой.

Операции смены регистраторов

При Совете ОПРИ создана рабочая группа для реализации третьего из шести запланированных проектов разработки политики, направленного на анализ различных аспектов изменения регистраторов. Эта рабочая группа, ПИР (часть Б), занимается решением пяти проблем, сосредоточив свое внимание на вопросах, связанных перехватом доменных имен, срочным возвратом неправильно переданного имени и «заблокированным» состоянием. РГ по вопросам ПИР (часть Б) опубликовала свой предварительный отчет 29 мая http://www.icann.org/en/announcements/announcement-05jul10-en.htm). Данный отчет содержит, помимо прочего, предложение по политике ускоренной отмены передачи и предложение запросить отчет о проблемах, касающихся требования использовать WHOIS с расширенным набором

данных для всех рДВУ. После закрытия 8 августа периода общественного обсуждения РГ проанализирует полученные комментарии общественности и приступит к окончательной доработке отчета для его представления на рассмотрение Совета ОПРИ.

Злоупотребления при регистрации

Перед рабочей группой по вопросам политики борьбы со злоупотреблениями при регистрации, которая начала свою деятельность в феврале 2009 г., была поставлена задача более тщательного изучения политики борьбы со злоупотреблениями при регистрации. РГ по вопросам ПБЗР обсудила такие вопросы, как определение различий между злоупотреблениями при регистрации и злоупотреблениями при использовании доменных имен, определение существующих злоупотреблений, идентификация возможных выгод и недостатков использования более универсального подхода при заключении договоров, а также возможные области (если таковые имеются), в которых следует формулировать политику ОПРИ по борьбе со злоупотреблениями при регистрации. РГ по вопросам ПБЗР представила свой итоговый отчет Совету ОПРИ 29 мая 2010 г. [http://www.icann.org/en/announcements/announcement-29may10-en.htm]. В этот отчет включены конкретные рекомендации по борьбе со злоупотреблениями при регистрации доменных имен в зоне рДВУ. В отчет включены рекомендации в отношении следующих проблем.

- *Киберсквоттинг: рекомендуется инициировать процесс разработки политики для изучения текущего состояния Единых правил рассмотрения споров о доменных именах (UDRP).*
- *Проблемы доступа к WHOIS: осуществляется поиск путей обеспечения доступности данных WHOIS с требуемой надежностью, возможностью доступа в принудительном порядке и постоянством; и направлен запрос отделу выполнения договорных обязательств ICANN на публикацию дополнительных данных о доступности WHOIS.*
- *Злонамеренное использование доменных имен: рекомендуется разработать передовые методы,*

чтобы помочь регистраторам и реестрам в решении проблем незаконного использования доменных имен.

- *Фальшивые уведомления о возобновлении: отделу выполнения договорных обязательств ICANN рекомендуется принять возможные принудительные меры.*
- *Мошеннические перекрестные регистрации ДВУ: рекомендуется согласовать мониторинг и исследование с сообществом.*
- *Единообразие контрактов: рекомендуется создать отчет о проблемах для оценки необходимости разработки минимально необходимых положений по предотвращению злоупотреблений при регистрации для всех соглашений, входящих в сферу деятельности ICANN.*
- *Практические методы в масштабе ОПРИ для сбора и распространения передовых практических методов и для обеспечения универсальности отчетности.*
- *Опережающая регистрация доменных имен*
- *Обманное использование доменных имен*
- *Вводящие в заблуждение или оскорбительные доменные имена*

При рассмотрении рекомендаций Совет ОПРИ принял решение сформировать проектную группу для разработки проекта предполагаемого подхода к рекомендациям, содержащимся в отчете, который может содержать сроки формирования групп для обсуждения некоторых рекомендаций из итогового отчета, а также порядок рассмотрения тех рекомендаций, по которым не было достигнуто единогласное мнение.

Восстановление доменных имен с истекшим сроком действия: Совет ОПРИ инициировал ПРП по восстановлению доменных имен с истекшим сроком действия в мае 2009 г. Эта рабочая группа решает вопросы о том, в какой мере владельцы регистрации могут заявлять о своих правах на доменные имена после истечения срока их действия. Рассматривается вопрос, адекватна ли текущая политика регистраторов по обновлению, передаче и удалению доменных имен после истечения срока их действия.

Улучшения CAP: Правление ICANN утвердило пересмотренное Соглашение об аккредитации регистраторов (CAP) в мае 2009 г. (http://www.icann.org/en/topics/raa/). Новое CAP расширяет комплексную проверку регистраторов и аффилированных с ними лиц, возможности идентификации регистраторов, которые могут быть вовлечены в кибресквоттинг или иную злонамеренную деятельность, расширяет требования к WHOIS и обязательствапоставщиков услуг конфиденциальной регистрации и регистрации через доверенных лиц, а также требования к определению канала связи регистратора для борьбы со злоупотреблениями с целью получения отчетов о случаях злонамеренного поведения с использованием DNS. *Представители правоохранительных органов, РКК и другие группы заинтересованных сторон принимают участие в поиске путей дальнейшего улучшения CAP (см. http://www.icann.org/en/announcements/announcement-28may10-en.htm) и представили свои предложения по внесению изменений на конференции ICANN в Брюсселе, состоявшейся в июне 2010 г.*

Интернационализированные регистрационные данные: В настоящее время отсутствуют стандарты или руководства по определению состава и отображения данных регистрации интернационализированных доменов. Для изучения возможности и целесообразности разработки технических требований отображения для работы с интернационализированными регистрационными данными Правлением ICANN была создана объединенная рабочая группа ОПРИ и ККБС. С целью обеспечения как можно большего вклада сообщества в обсуждение данного вопроса в ходе своей работы группа будет заниматься привлечением комментариев со стороны других заинтересованных субъектов, в том числе операторов нДВУ, ОПРИ, ОПА, РКК и ПКК. Первоначальный набор задач РГ-ИРД состоит в обеспечении понимания и достижения консенсуса по типам, видам и кодировкам регистрационных данных, которые должны собирать, отображать и поддерживать стороны, связанные договорными обязательствами.

6. Планы ICANN по повышению безопасности, стабильности и отказоустойчивости на 2011 ФГ

Процессы стратегического и оперативного планирования направляют деятельность ICANN в отношении повышения безопасности, стабильности и отказоустойчивости и определяют ресурсы, выделяемые на реализацию этих усилий. В 2011 ФГ деятельность ICANN будет включать ряд важнейших инициатив, таких как:

- ***Деятельность IANA*** — обеспечение поддержки, обучения и подготовки к внедрению DNSSEC на корневом уровне, как записано в стратегическом плане ICANN на 2010–2013 гг., а также улучшение управления корневой зоной посредством автоматизации и улучшение методов аутентификации обмена информацией с управляющими ДВУ.
- ***Операции корневых серверов 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*** — обеспечение дальнейшей безопасности деятельности в ходе оценки заявок на новые рДВУ и ИДИ. ICANN продолжит доработку плана бесперебойной работы реестров рДВУ и тестирование системы ответственного хранения данных.
- ***Реестры нДВУ*** — ICANN расширит сотрудничество в области доработки программы наращивания потенциала DNS, включая совместное планирование реагирования на нападения и чрезвычайные происшествия (ПРНЧП) и программу обучения операциям реестра, введенную в сотрудничестве с ОПНИ и региональными ассоциациями ДВУ.
- ***Выполнение договорных обязательств*** — ICANN продолжит расширение масштабов деятельности по обеспечению выполнения договорных обязательств, связанных с рДВУ, и начнет проведение аудиторских проверок договорных сторон в рамках исполнения поправок к САР от 2009 года и определение потенциальной возможности злонамеренного поведения договорных сторон для принятия исправительных мер.

- ***Реагирование на злоупотребления системой доменных имен*** — ICANN продолжит развитие усилий по сотрудничеству, направленных против злонамеренного поведения, связанного с использованием DNS, и содействие обмену информацией для обеспечения эффективного реагирования.
- ***Внутренняя безопасность ICANN и обеспечение непрерывности деятельности*** — ICANN продолжит реализацию программ обеспечения безопасности в рамках общего управления корпоративными рисками и кризисными ситуациями, а также программ обеспечения непрерывности деятельности. Основное внимание будет уделено внедрению документально оформленных планов и вспомогательных процедур.
- ***Обеспечение повсеместного участия и сотрудничества*** — ICANN продолжит расширение партнерских отношений с Комиссией по технологиям Интернета (IETF), Обществом Интернета (ISOC), региональными интернет-реестрами и группами операторов сетей, операционным, аналитическим и исследовательским центром DNS (DNS-OARC) и форумом групп быстрого реагирования (FIRST). ICANN также будет принимать участие в межнациональных диалогах, направленных на расширение понимания трудностей в сфере безопасности, стабильности и отказоустойчивости, стоящих перед экосистемой Интернета, и способов устранения этих трудностей при участии большого количества заинтересованных сторон.

Полный перечень проектов приведен ниже. В приложении A указаны конкретные цели, участники, результаты и ресурсные требования, запланированные на 2011 ФГ.

6.1 Ключевые функции DNS и системы адресации

6.1.1 Деятельность IANA

ICANN продолжит руководство функциями IANA и работу по улучшению показателей деятельности этого агентства в сотрудничестве с Министерством торговли США, корпорацией VeriSign, РИР и операторами ДВУ.

Среди конкретных инициатив по улучшению функций IANA можно перечислить следующие:

- Улучшение управления корневой зоной посредством автоматизации (программное обеспечение eIANA/RZM); улучшение аутентификации обмена информацией с управляющими ДВУ; пересмотр механизмов и практических методов с учетом соображений безопасности и оптимизации.
- Поддержка разработки и внедрения сертифицированного выделения и назначения IP-адресов через инфраструктуру ИОКР или другие механизмы, принятые РИР и сообществом маршрутизации Интернета при постоянной поддержке со стороны рабочей группы IETF по вопросам защищенного междоменного репозитория (SIDR).
- Сотрудничество с техническими и операционными сообществами по определению, анализу и возможному внедрению дополнительных технических требований или стандартов для повышения безопасности, стабильности и отказоустойчивости DNS.

В рамках общих мер по повышению отказоустойчивости в январе 2010 г. ICANN провела учения по обеспечению непрерывности деятельности IANA, проверив работоспособность передачи услуг IANA в случае отказа из Марина дель Рей, Калифорния, в Рестон, Вирджиния. Эти учения продемонстрировали возможности IANA по переключению при отказе и механизмы обмена информацией, обеспечивающие доступность услуг IANA. ICANN повысит отказоустойчивость услуг IANA в 2010–2011 гг.

6.1.2 Операции DNS

ICANN, Министерство торговли США и корпорация VeriSign в 2010 г. достигли существенного рубежа, внедрив DNSSEC в корневой зоне. Согласно приоритетам, сформулированным в стратегическом плане на 2010–2013 гг., ICANN продолжит усилия по поддержке внедрения DNSSEC операторами ДВУ и другими субъектами в 2011 ФГ.

ICANN также будет осуществлять ряд проектов, позволяющих расширить DNSSEC по всей DNS, сотрудничая с экспертами в области DNS и опытными операторами. ICANN обеспечит включение в свою программу механизмов изменения регистраторов и создания необходимых для этого счетов ответственного хранения, а также продолжит обсуждения конкретных вопросов внедрения с заинтересованными сторонами. ICANN будет продолжать поддержку репозитория

отметок о доверии IANA 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 путем подписания зон, управляемых корпорацией (включая icann.org и iana.org), и будет содействовать распространению полученного опыта среди субъектов, вовлеченных во внедрение DNSSEC.

ICANN стремится способствовать реализации более надежных механизмов координации в рамках сообщества операторов корневой зоны в отношении мер, способствующих безопасности, стабильности и отказоустойчивости. В качестве оператора корневого сервера «L» корпорация ICANN планирует сотрудничать с прочими операторами корневой зоны по инициации добровольных усилий, направленных на осуществление планирования и проведение учений в целях повышения отказоустойчивости систем корневых серверов на случай ряда напряженных чрезвычайных обстоятельств.

ICANN планирует продолжать улучшение работы корневого сервера «L». Кроме того, ICANN привлекла центр DNS-OARC к исследованию влияния изменений, включая ввод новых рДВУ и ИДИ, внедрение IPv6 и возможное внедрение подписей DNSSEC в корневой зоне, на функционирование отдельной секции корневых серверов на основе модели корневой зоны «L». В более широком смысле ККСКС и ККБС проводят совместное исследование безопасности и стабильности корневых серверов в свете предполагаемых изменений, описанных в разделе 6.6.

6.2 Взаимоотношения с реестрами ДВУ и регистраторами

6.2.1 Реестры рДВУ

ICANN продолжит координацию договорных отношений, связанную с операциями рДВУ, включая приложения для проверки новых услуг через процесс оценки услуг реестра (ПОУР). После внедрения процесса ввода новых рДВУ ICANN ожидает включения в состав проверок предложений с требованием 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 путем проведения региональных семинаров ICANN для реестров и

регистраторов, участия в ряде форумов сообщества и распространения информации через собственный веб-сайт. В 2010 г. ICANN ввела расширенную отчетность по данным реестров рДВУ на своей сводной панели для использования сообществом (http://www.icann.org/idashboard/public/).

6.2.2 Новые рДВУ

На протяжении всего грядущего года основное внимание в сфере безопасности, стабильности и отказоустойчивости будет уделяться 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 всей системы корневых серверов ряда возможных изменений в DNS, включая внедрение новых рДВУ и ИДИ, а также возможное внедрение подписей DNSSEC для корневой зоны. Ожидается, что отчет этих консультативных комитетов будет представлен в 2010 г. В рамках процесса ввода новых рДВУ корпорация ICANN также сформулирует положения по оценке кандидатов, чтобы убедиться, что они способны реализовывать технически безопасные операции, соответствующие положениям WHOIS, а также обеспечивать приемлемое планирование на случай чрезвычайных происшествий и защиту владельцев регистраций. ICANN продолжит дорабатывать план обеспечения непрерывности деятельности реестров нДВУ и программу учений. ICANN также обеспечит создание и безопасную эксплуатацию автоматизированной системы подачи заявок для кандидатов на получение 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 символами местного языка, были безопасными, стабильными и отказо-устойчивыми. ICANN поддерживает работу по обновлению Руководства по ИДИ для операторов ДВУ с ИДИ и эксплуатации ИДИ второго уровня. ICANN будет как и раньше способствовать усилиям реестров по сотрудничеству с поставщиками в обеспечение создания таблиц ИДИ, максимально ограничивающих конфликты строк и путаницу и сокращающих возможности для злоупотребления системой в недобросовестных целях. Для лиц, заинтересованных в том, чтобы стать оператором ДВУ с ИДИ, и нуждающихся в

содействии и навыках в этой сфере, будет предоставлена функция компетентной поддержки в области ИДИ.

ICANN будет также сотрудничать с экспертами в целях обеспечения стабильности ввода ДВУ с ИДИ для тех стран и территорий, где имеется несколько подходящих языков или шрифтов и необходима синхронизация внедрения. Сюда также относится сотрудничество в целях поддержки внедрения ИДИ с такими заинтересованными сторонами, как разработчики браузеров и приложений, операторы реестров ИДИ и прочие субъекты.

6.2.4 нДВУ

ICANN продолжит свои усилия, связанные с повышением безопасности, стабильности и отказоустойчивости нДВУ, путем сотрудничества с операторами нДВУ. В ближайшем году эта деятельность будет сосредоточена на доработке совместной программы наращивания потенциала DNS, включающей программу семинаров по совместному планированию реагирования на нападения и чрезвычайные происшествия (ПРНЧП), введенную в сотрудничестве с ОПНИ и региональными ассоциациями ДВУ. Программа наращивания потенциала DNS сосредоточена на повышении безопасности и отказоустойчивости посредством упреждающего планирования и повышенной способности к реагированию на полный спектр деструктивных угроз и рисков. В грядущем году эта программа расширится и будет включать техническое обучение, направленное на укрепление безопасности и отказоустойчивости в ответ на растущие угрозы и на предоставление помощи в разработке программ проведения учений и оценки планирования систем безопасности и реагирования на чрезвычайные происшествия.

6.2.5 Регистраторы

Сообщество предваряет дальнейшее обсуждение усовершенствования требований к аккредитации регистраторов и ответственному хранению данных через улучшение 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, ведется работа по усовершенствованию процедур оформления заявок на аккредитацию, повышению требований к желающим заключить CAP и ужесточению правил дисквалификации, 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 обмениваться передовым опытом в отрасли, и начнет реализовывать новые каналы связи, призванные помочь регистраторам своевременно сообщать о критических угрозах безопасности и реагировать на них.

6.2.6 Выполнение договорных обязательств

ICANN продолжит расширять масштаб мер по обеспечению выполнения договорных обязательств. Эта деятельность будет включать аудиторские проверки договорных сторон в рамках внедрения CAP 2009. Кроме того, сотрудники отдела выполнения договорных обязательств будут работать совместно с сотрудниками отдела безопасности ICANN над выявлением партнеров по договорам, подозреваемых в злонамеренной деятельности. В случаях, когда партнеры по договорам ведут злонамеренную деятельность, могут быть приняты меры по обеспечению выполнения договорных обязательств. Во всех остальных случаях для адекватного решения вопросов такого рода будут оповещаться правоохранительные и прочие соответствующие органы.

Отдел выполнения договорных обязательств провел исследования по оценке точности контактных сведений, содержащихся в данных WHOIS системы рДВУ, и степени, в которой владельцы регистраций используют услуги обеспечения конфиденциальности и регистрации через доверенных лиц для сокрытия своей личности. Стремясь стимулировать выполнение договорных обязательств и обеспечить доверие со стороны общественности, отдел выполнения договорных обязательств разрабатывает систему открытой публикации данных о лицах, в полной мере выполняющих свои обязательства. Эта система находится на ранней стадии разработки, и перед ее внедрением будут проведены консультации с сообществами регистраторов и реестров.

6.2.7 Совместное реагирование на злоупотребления системой доменных имен

Сотрудники ICANN также продолжат развитие совместных проектов, возникших в ответ на недавние события с участием системы доменных имен, произошедшие с конца 2008 года, таких как меры принятые в связи с бот-сетью Szirbi и червем Conficker в конце 2008 — начале 2009 года. ICANN считает, что в подобном сотрудничестве должны участвовать реестры и регистраторы DNS, сообщество исследований в области безопасности и поставщики программного обеспечения и антивирусных программ. В частности, ICANN планирует работать совместно с сообществами реестров и регистраторов над развитием сотрудничества в сфере борьбы со зловредным ПО, 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 обеспечит возможность открытого обсуждения своих процедур реализации совместного реагирования. Эти процедуры будут представлены на утверждение Правления. Такое сочетание подходов обеспечит способность ICANN реагировать на запросы любых заинтересованных сторон, которым может потребоваться ее участие и сотрудничество.

6.2.8 Обеспечение общей безопасности DNS

Сотрудники ICANN будут стремиться развивать результаты симпозиумов по безопасности, стабильности и отказоустойчивости DNS, прошедших в феврале 2009 г. и в феврале 2010 г., путем 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 всей DNS, и преумножению возможностей сотрудничества, не теряя из виду решение задач по обеспечению безопасности и стабильности DNS в развивающемся мире. ICANN также планирует сотрудничать с центром DNS-OARC и форумом групп быстрого реагирования и отделов безопасности (FIRST), уделяя основное внимание подготовке эффективных ответов на значительные происшествия и события в сообществе DNS. Кроме того, сотрудники ICANN будут по-прежнему следить за развитием планов по формированию системы назначения

имен объектам (ONS) и за тем, как такие планы могут включать DNS для обеспечения раннего определения некоторых потенциальных проблем, связанных с безопасностью, стабильностью и отказоустойчивостью.

6.3 Глобальная разъяснительная работа в сфере безопасности

6.3.1 Расширение существующих партнерств

Суть стратегии глобального участия ICANN в деятельности по обеспечению безопасности, стабильности и отказоустойчивости заключается в том, чтобы развивать и использовать существующие результаты работы, осуществляемой отделом глобальных партнерств, и еще более расширять крепкие партнерские отношения. На 2011 финансовый год с этими партнерами запланированы следующие проекты.

- ***Общество Интернета (ISOC)*** — ICANN планирует продолжать сотрудничество в рамках текущей совместной программы ISOC и ICANN по обеспечению обучения операторов ДВУ, а в дополнительные планы входит техническое обучение методам повышения безопасности и смягчения последствий кибератак и нарушений в работе.
- ***DNS-OARC*** —ICANN продолжит сотрудничество с центром DNS-OARC и другими заинтересованными сторонами в рамках поддержки стратегических инициатив по БСО и концепции DNS-CERT. ICANN также взаимодействует с различными организациями в целях проведения образовательных мероприятий, нацеленных на улучшение понимания работы систем уникальных идентификаторов, роли корпорации и трудностей, возникающих при управлении рисками для этих систем.

6.3.2 Коммерческие предприятия

ICANN будет развивать результаты прошедших в феврале 2009 г. и в феврале 2010 г. симпозиумов 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.

6.3.3 Участие в международном диалоге по кибербезопасности

ICANN будет принимать участие в данных диалогах с целью формирования четкого понимания своей конкретной роли и вклада. В этой сфере ICANN предусмотрела на следующий год следующие конкретные мероприятия.

- ***Форум групп быстрого реагирования и отделов безопасности (FIRST)*** — ICANN и FIRST в марте 2010 г. провели совместный семинар по кибербезопасности в Найроби, Кения, для африканских групп быстрого реагирования. ICANN сотрудничает с FIRST при проведении опроса групп быстрого реагирования на нарушения компьютерной безопасности в 2011 ФГ и принимает участие в программах FIRST.
- ***Европейское агентство по сетевой и информационной безопасности (ENISA)*** —ICANN планирует сотрудничать с ENISA в рамках проведения европейских учений в киберпространстве и мероприятий по реагированию на происшествия в киберпространстве.
- ***Форум управления Интернетом (IGF)*** — ICANN будет принимать участие в собрании IGF в Вильнюсе, Литва, которое запланировано на сентябрь 2010 г., и выступает в поддержку принятия решения на Генеральной Ассамблее Организации Объединенных Наций о продолжении работы IGF.

ICANN будет активно использовать возможности сотрудничества с другими организациями и научными учреждениями для достижения лидерства в определении задач, связанных с безопасностью, стабильностью и отказоустойчивостью.

ICANN также планирует сотрудничать с ОПА (а через ОПА — с ОНР и РИР) и участвовать в деятельности по решению вызывающих обоюдную озабоченность вопросов обеспечения безопасности, стабильности и отказоустойчивости. Сотрудники ICANN будут стремиться заручаться мнением ОНР относительно конкретных совместных проектов по расширению возможностей обеспечения безопасности, стабильности и отказоустойчивости DNS. Эти дискуссии будут в том числе направлены на понимание намерений ОНР относительно возможных злоупотреблений наследием адресного пространства IPv4 и потенциальной необходимости

формулирования региональной и, возможно, глобальной политики для решения выявленных проблем.

6.4 Корпоративная безопасность ICANN и операции по обеспечению непрерывности деятельности

Сотрудники ICANN обеспечат реализацию программ по безопасности в рамках общего управления корпоративными рисками и кризисными ситуациями, а также программ обеспечения непрерывности деятельности. Основное внимание по-прежнему будет уделяться созданию крепкого фундамента в виде документально оформленных политик, процессов и вспомогательных процедур. Последние инициативы были сосредоточены на улучшении управления рисками ICANN на уровне предприятия и обеспечении непрерывности деятельности, включая разработку официальных планов сохранения непрерывности деловых операций ICANN и управления кризисами, а также проведение внутренних учений в ICANN в совокупности с прочими мероприятиями, подразумевавшими тренировки для поддержания непрерывности функционирования рДВУ и подготовку к конференциям. ICANN стала инициатором использования физически распределенных альтернативных объектов для осуществления операций с целью улучшения непрерывности деловых операций и расширения возможностей ликвидации последствий чрезвычайных ситуаций в ИТ-инфраструктуре корпорации.

В рамках текущих операций в 2010 г. сотрудники ICANN продолжают улучшать весь спектр корпоративных процессов в сфере информации, персонала и безопасности. Как и в случае с управлением риском и планированием непрерывности, основное внимание будет уделено созданию прочной основы в виде документально оформленных планов и вспомогательных процедур. Конкретные инициативы по повышению безопасности ICANN, находящиеся в 2010 г. в процессе реализации, включают усовершенствование элементов логического и физического контроля доступа, изменение механизмов управления, процедуры ведения журналов (аудита) и резервного копирования данных, обучение персонала с целью повышения осведомленности в вопросах безопасности, наращивание возможностей реагирования на происшествия и повышение безопасности мобильных устройств. Подготовлены документально оформленные планы обеспечения безопасности персонала и

проведения международных конференций ICANN. Независимая проверка и анализ этих планов запланирована на конец 2010 г. ICANN обеспечит разработку и развертывание ИТ-средств для развития сотрудничества в рамках сообщества и проведения разъяснительной работы, предусмотрев необходимые элементы управления безопасностью.

ICANN планирует провести внешний анализ и проверку своих программ по обеспечению безопасности и непрерывности деятельности, осуществлявшихся в течение второй половины 2010 г.

6.5 Организации поддержки и консультативные комитеты ICANN

ККБС планирует сосредоточить в будущем свои усилия на развертывании DNSSEC, защите регистрации доменов и сокращении неправомерного использования доменных имен, а также на обеспечении стабильности системных адресов.

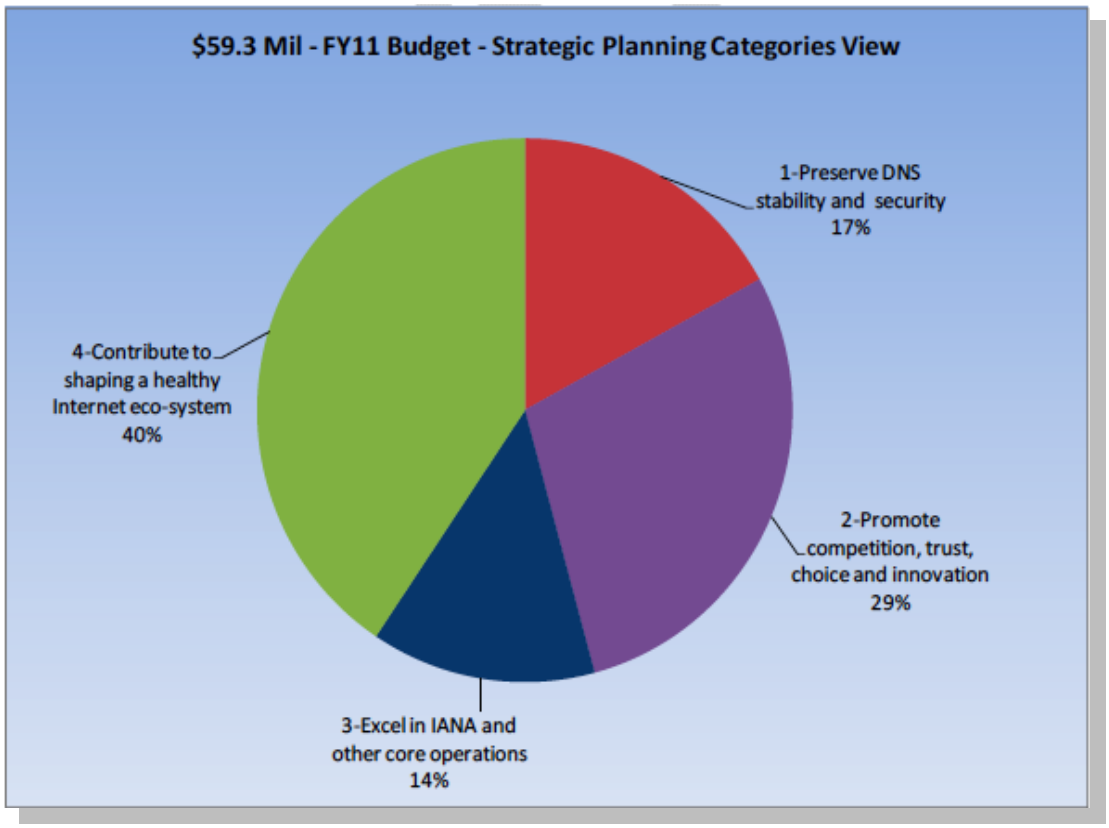
В январе 2009 г. Совет ОПРИ опубликовал для открытого обсуждения и дальнейших действий Совета предварительный отчет по хостингу «Fast Flux» и также рассматривает многочисленные возможные сопутствующие исследования WHOIS. При Совете ОПРИ создана рабочая группа для реализации второго из шести запланированных проектов разработки политики, направленного на анализ различных аспектов изменения регистраторов. ОПРИ создала рабочую группу по вопросам злоупотреблений при регистрации и рассматривает инициативу, связанную с восстановлением доменных имен после истечения срока их действия. С целью собрать вместе широкий круг субъектов ICANN, заинтересованных в решении данных вопросов, в повестку дня нескольких открытых международных конференций ICANN были включены развернутые семинары по электронной преступности и злоупотреблениям при регистрации (в Мехико, Сеуле, Найроби, Брюсселе).

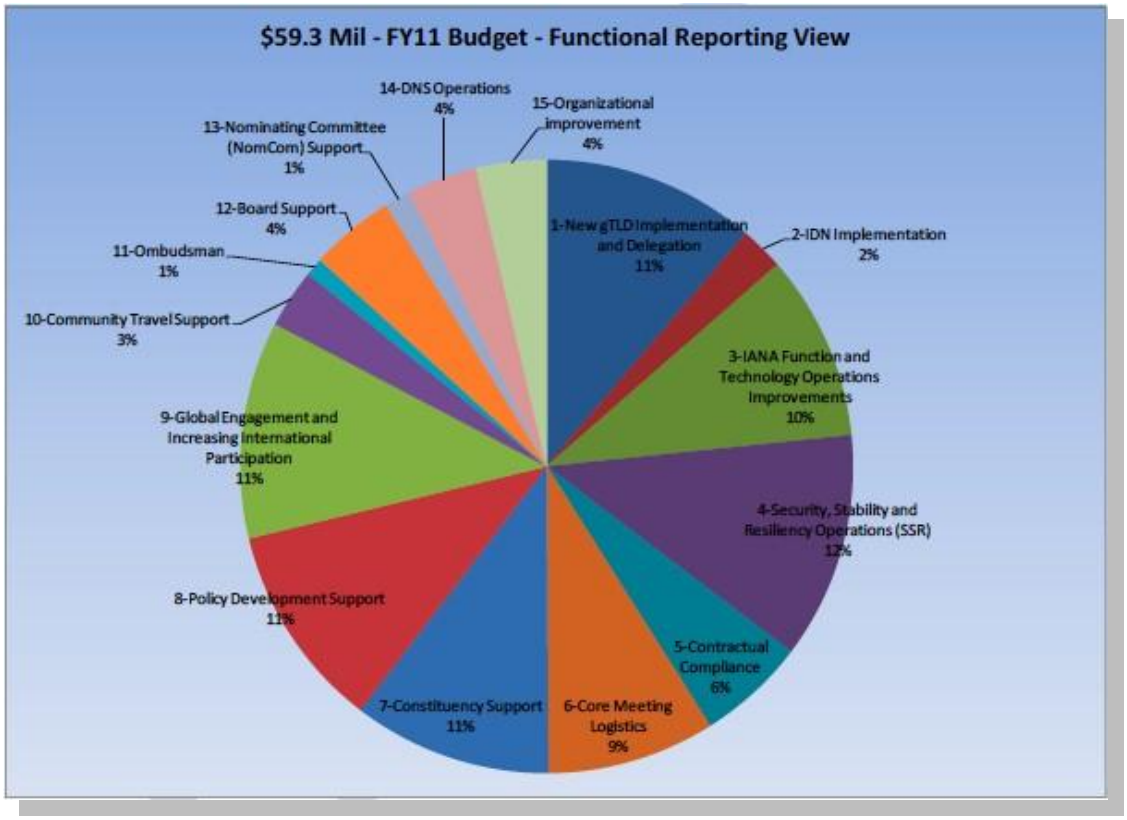
7. Заключение

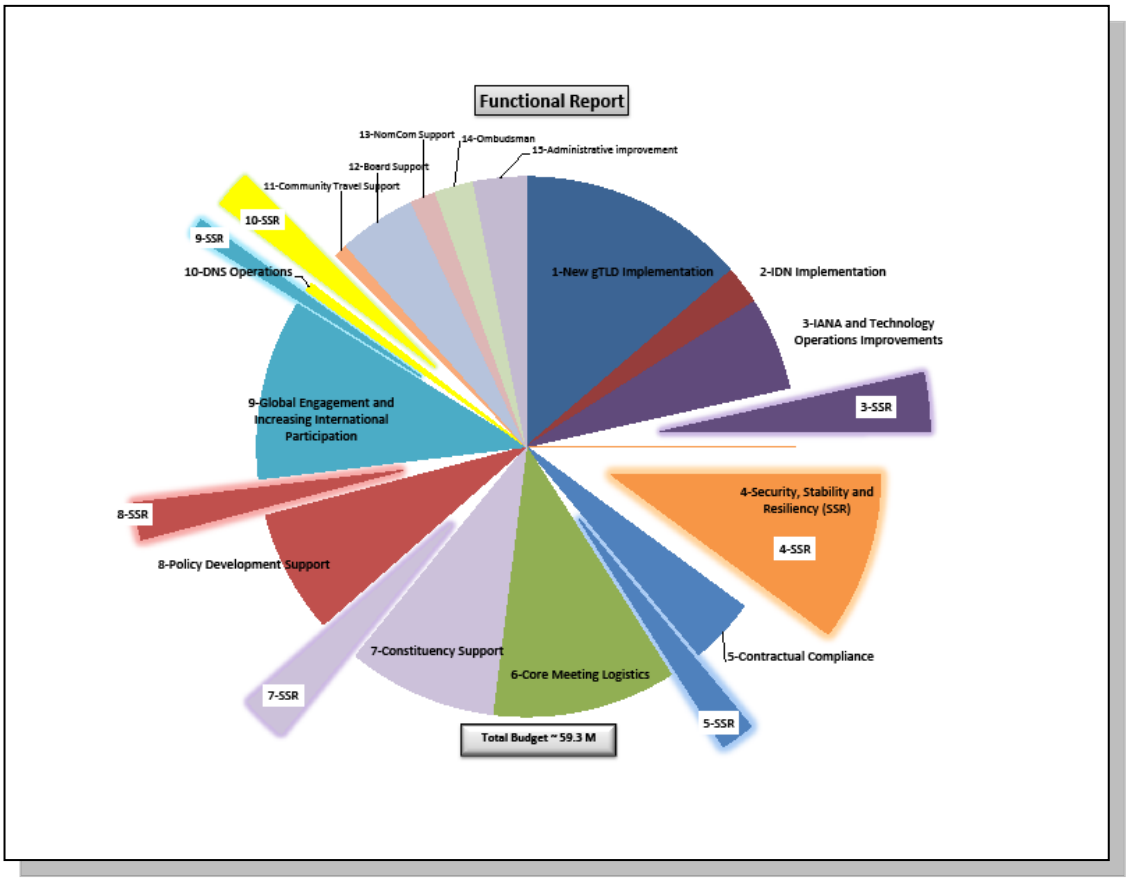
ICANN осознает, что важнейшим аспектом ее задачи по формированию доверия общественности является вклад программ и проектов корпорации в превращение систем уникальных идентификаторов в ключевой аспект более безопасной, стабильной и отказоустойчивой интернет-среды. Трудности растут, и усилия ICANN в этом направлении становятся все более напряженными. ICANN также признает ограничения своей роли и ресурсов и планирует свою стратегию в этой сфере с упором на сотрудничество. Интернет представляет собой глобальную среду, опирающуюся на стимулирование инноваций и координирование с привлечением большого количества заинтересованных сторон. В основе вклада ICANN в укрепление безопасности, стабильности и отказоустойчивости систем уникальных идентификаторов будет лежать такой же подход.

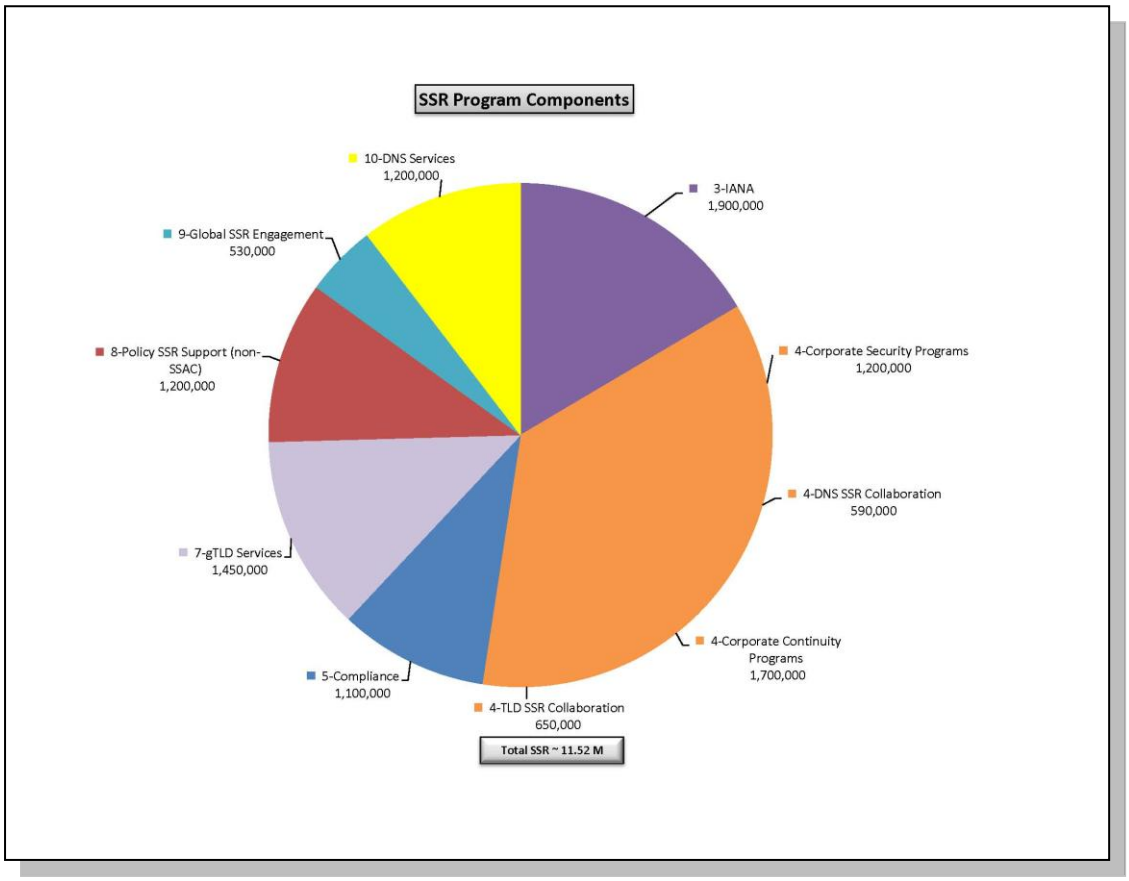
С момента своего создания ICANN осуществляет программы и проекты, направленные на улучшение безопасности, стабильности и отказоустойчивости Интернета, включая усилия, связанные с ключевыми функциями DNS и системы адресации; сотрудничество с сообществами реестров и регистраторов ДВУ; взаимодействие с ОНР и РИР; программы обеспечения корпоративной безопасности и непрерывности работы; деятельность организаций поддержки и консультативных комитетов, а также участие в глобальных и локальных проектах по безопасности, стабильности и отказоустойчивости Интернета. Задачей этой первой редакции плана является обеспечение основы 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 оперативного планирования ICANN, позволяя проектам корпорации сохранять актуальность и обеспечивая применение ее ресурсов для выполнения наиболее важных обязанностей и вкладов.

Приложение A — Выделение ресурсов на БСО в 2011 ФГ




$59.3 Mil - FY11 Budget - Functional Reporting View
1-New gTLD Implementation and Delegation 11%
2-IDN Implementation 2%
3-IANA Function and Technology Operations Improvements 10%
4-Security, Stability and Resiliency Operations (SSR) 12%
5-Contractual Compliance 6%
6-Core Meeting Logistics 9%
7-Constituency Support 11%
8-Policy Development Support 11%
9-Global Engagement and Increasing International Participation 11%
10-Community Travel Support 3%
11-Ombudsman 1%
12-Board Support 4%
13-Nominating Committee (NomCom) Support 1%
14-DNS Operations 4%
15-Organizational improvement 4%


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
5-Contractual Compliance
7-Constituency Support
6-Core Meeting Logistics
7-SSR
5-SSR
Total Budget ~ 59.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-Corporate Security Programs
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
4-Corporate Continuity Programs
1,700,000
5-Compliance
1,100,000
4-TLD SSR Collaboration
650,000
Total SSR ~ 11.52 M

Обзор основных компонентов программы ICANN по обеспечению безопасности, стабильности и отказоустойчивости (БСО)

- IANA — 1,9 млн. долл. США
- Услуги DNS — 1,2 млн. долл. США
- Сотрудничество по БСО DNS — 590 тыс. долл. США
- Услуги рДВУ — 1,45 млн. долл. США
- Соблюдение договорных обязательств — 1,1 млн. долл. США
- Сотрудничество по БСО ДВУ — 650 тыс. долл. США
- Глобальное взаимодействие по БСО — 530 тыс. долл. США
- Программы корпоративной безопасности — 1,2 млн. долл. США
- Программы непрерывности деятельности корпорации — 1,7 млн. долл. США
- Поддержка политики по БСО (не ККБС) — 550 тыс. долл. США
- Поддержка ККБС — 650 тыс. долл. США

ИТОГО БСО — 11,52 млн. долл. США

Безопасность, стабильность и отказоустойчивость Агентства по распределению номеров Интернета (IANA)

Цели

- Автоматизация важнейших элементов процессов изменения в корневой зоне
- Управление DNSSEC
- Пробное внедрение ИОКр
- Непрерывность бизнеса

Результаты (этапы)

- Внедрение автоматизированного метода корневой зоны (RZM) (зависит от партнеров: NTIA и VeriSign)
- Внедрение подписи DNSSEC для .ARPA (дата зависит от результатов согласования с IAB и NTIA)
- Согласование с тестировщиками ИОКр
- План непрерывности деятельности IANA (проверен в январе 2010 г., постоянная проверка запланирована в 2011 ФГ)

Ключевые заинтересованные стороны

- IANA, Отдел безопасности, ИТ
- Министерство торговли и Правительство США, Verisign
- ККБС, ККСКС
- IETF, сообщество операторов DNS
- РИР, сообщество по функционированию систем маршрутизации

Ресурсы

- Кадровые — 6,5 сотрудников на полную ставку (СПС) (в том числе 2,5 СПС для соответствующего ИТ и прочего вспомогательного персонала).
- Финансовые — 1,9 млн. долл. США на поддержку СПС, поддержку персонала и командировок; профессиональные услуги; разработку приложений.

Операции DNS ICANN

Цели

- Мероприятия DNSSEC и периодическая смена ключей
- Внедрение подписей ICANN для .arpa и других зон
- Репозиторий отметок о доверии (РОД)
- Безопасная и отказоустойчивая эксплуатация корневого сервера «L»

Результаты (этапы)

- Смена ключей в 2011 ФГ на объектах в Кульперере и Лос-Анджелесе
- Подписанные с использованием DNSSEC зоны ICANN
- Функционирование репозитория отметок о доверии
- Усовершенствование зоны корневого сервера «L»

Ключевые заинтересованные стороны

- Группа эксплуатации DNS ICANN, группы ИТ
- Сотрудники IANA ICANN, Министерство торговли, VeriSign
- Отдел безопасности ICANN

Ресурсы (2011 ФГ)

Кадровые — 7,0 СПС (включая соответствующий ИТ и прочий вспомогательный персонал)

Финансовые — 1,2 млн. долл. США на поддержку СПС; запланированные капитальные вложения в службы резервного копирования; DNSSEC, корневой сервер «L», модернизацию; резервные объекты; профессиональные услуги и командировки

Услуги ICANN для реестров и регистраторов рДВУ (услуги)

Цели

- Обеспечить решение вопросов БСО при внедрении новых рДВУ и ИДИ
- Продолжить совершенствование процесса ответственного хранения данных и плана обеспечения целостности рДВУ
- Реализация процессов ПОУР и ГТОУР

Результаты

- Улучшенный в отношении БСО процесс внедрения рДВУ
  - Завершение масштабирования корневой зоны (в 2011 ФГ)
  - Улучшенное руководство для кандидатов (ноябрь 2010 г.)
- Учения по передаче данных на ответственное хранение (август-ноябрь 2010 г.)
- Запрос информации (RFI) по ДВУВСБ (сентябрь-ноябрь 2010 г.)
- Положения договоров по злонамеренному поведению

Ключевые заинтересованные стороны

- Реестры и регистраторы
- Персонал отдела услуг ICANN
- Персонал отдела безопасности и обеспечения непрерывности деятельности ICANN
- ОПРИ и ККБС

Ресурсы (2011 ФГ)

Кадровые — 2,75 СПС

Финансовые — бюджет новых рДВУ подлежит определению: включает часть расходов на оценочный персонал и поддержку деятельности, связанной с новыми рДВУ и ИДИ, включая безопасность СЗД; средства, выделенные на ПОУР и ГТОУР; поддержку тестирования и подготовки к чрезвычайным происшествиям; командировки и поддержку сотрудников

Соблюдение договорных обязательств (услуги)

Цели

- Улучшенная процедура обеспечения соблюдения договорных обязательств ICANN
- Улучшенная система претензий и WDPRS
- Повышенная точность данных WHOIS

Результаты

- Проведение проверок в рамках внедрения CAP 2009
- Улучшения WDPRS (август-ноябрь 2010 г.)
- Дополнительные исследования WHOIS в зависимости от рекомендации Совета ОПРИ

Ключевые заинтересованные стороны

- Реестры и регистраторы рДВУ
- Сотрудники отдела соблюдения договорных обязательств ICANN
- Персонал отдела безопасности и обеспечения неприрывности деятельности ICANN

Ресурсы (2011 ФГ)

Кадровые — 3 СПС

Финансовые — 1,1 млн. долл. США на поддержку СПС, персонала и командировок; профессиональные услуги по проведению исследований и поддержке системных улучшений;

Сотрудничество в области безопасности, стабильности и отказоустойчивости ДВУ
(безопасность)

Цели
- Доработка программы по наращиванию потенциала DNS
- Организация совместной программы технического обучения ISOC и ICANN
- Проведение семинаров по планированию учений ДВУ
- Определение показателей программы

Результаты (этапы)
- Проведение учебных курсов по ПРНЧП, запланированных на 2010 г.
- План совместных с ISOC курсов технического обучения, переход в 2010 г.
- Проведение семинаров по планированию учений ДВУ
- Прототипы параметров по результатам симпозиума DNS

Ключевые заинтересованные стороны
- Операторы нДВУ
- ОПРИ, региональные операторы ДВУ
- ISOC и NSRC
- Сотрудники ICANN

Ресурсы (2011 ФГ)

Кадровые — 1 СПС

Финансовые — 650 тыс. долл. США на СПС, поддержку персонала и командировки; профессиональные услуги по разработке и проведению обучающих программ

Сотрудничество в области безопасности, стабильности и отказоустойчивости DNS
(безопасность)

Цели
- Установить механизмы совместного реагирования на злоупотребления DNS
- Обменяться важнейшими практическими методами в области БСО
- Провести в рамках сообщества симпозиум по рискам для DNS и сотрудничеству
- Укрепить сотрудничество в области БСО корневого сервера

Результаты (этапы)
- Схема сотрудничества и постоянное совместное с партнерами реагирование
- Проведение симпозиума и отчет о результатах (февраль и март 2010 г.)
- Отчет по оперативным учениям в корневой зоне (подлежит согласованию в 2010 г.)

Ключевые заинтересованные стороны
- ISOC, DNS-OARC, FIRST
- Сообщество корневых серверов
- Более широкое сообщество операций DNS
- Сотрудники ICANN
- ККСКС и ККБС

Ресурсы (2011 ФГ)

Кадровые —1,25 СПС

Финансовые — 590 тыс. долл. США на СПС, профессиональные услуги по поддержке порталов и сотрудничеству, командировки на мероприятия по поддержке

Программа корпоративной безопасности

(безопасность, ИТ, прочие сотрудники)

Цели

- Улучшить и реализовать программы в сфере безопасности ИТ, объектов и сотрудников
  - внедрить официальные планы
  - ввести подготовку в области безопасности
- Внедрить планы по безопасности перемещений и совещаний и планы реагирования на чрезвычайные происшествия

Результаты

- Проводить программы обучения в сфере безопасности (составляющая часть первичного обучения ICANN по состоянию на сентябрь 2009 г.)
- Внедрены улучшенные системы ИТ и контроля физического доступа (улучшенная ИТ-аутентификация в ключевых системах — осень 2009 г.)
- Провести учения по безопасности перемещений и совещаний (одно учение в четыре месяца)

Ключевые заинтересованные стороны

- Отдел безопасности и отказоустойчивости ICANN
- Отделы ИТ, IANA и операций DNS ICANN
- Отдел кадров ICANN
- Отдел международных конференций ICANN
- Прочий персонал ICANN

Ресурсы

Кадровые — 2 СПС (включая ИТ-поддержку безопасности)

Финансовые — 1,1 млн. долл. США, включая СПС, физические и ИТ-системы контроля доступа, профессиональные услуги по проведению обучения и проверок

Программа непрерывности деятельности корпорации

(персонал отдела безопасности, ИТ, прочие сотрудники)

Цели

- Улучшить программу непрерывности деятельности
  - Разработать официальный план
  - Создать безопасный центр обработки данных
  - Определить официальные программы учений и тренировок

Результаты

- Внутренний план обеспечения непрерывности бизнеса ICANN (октябрь 2010 г.)
- Повышение отказоустойчивости центра обработки данных
- Проведение учений по обеспечению непрерывности бизнеса и управлению кризисными ситуациями (октябрь 2010 г. — март 2011 г.)

Ключевые заинтересованные стороны

- Отдел безопасности ICANN
- Отделы ИТ, IANA и операций DNS ICANN
- Отдел кадров ICANN
- Отдел международных конференций ICANN
- Сотрудники ICANN

Ресурсы

Кадровые — 5 СПС (включая планирование и ИТ-персонал для центра обработки данных)

Финансовые — 1,7 млн. долл. США, включая СПС, капиталовложения в центр обработки данных, профессиональные услуги по проведению учений и проверок

Участие в глобальной деятельности по обеспечению безопасности, стабильности и отказоустойчивости

(глобальные партнерства и безопасность)

Цели

- Поддерживать партнерские отношения с ключевыми организациями (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Атлантическим советом)
- Продолжать участие в поддерживаемых IGO диалогах по кибербезопасности (ОЭСР, IGF и прочие)
- Сотрудничать с другими организациями по вопросам глобального реагирования на угрозы кибербезопасности

Результаты

- Проведение совместных мероприятий с партнерскими организациями (один раз в четыре месяца)
- Участие в форумах во всех крупных регионах (постоянное)
- Членство в форуме групп быстрого реагирования и отделов безопасности (FIRST)

Ключевые заинтересованные стороны

- Всемирные и международные организации
  - ISOC; IETF; ITU; IGF
- Форумы по кибербезопасности
- Правительства и коммерческие субъекты
- Сотрудники отдела глобальных партнерств ICANN и отдела безопасности

Ресурсы (2011 ФГ)

Кадровые — 1,5 СПС

Финансовые — 530 тыс. долл. США на СПС; поддержку персонала и командировок; финансирование форумов, проводимых или поддерживаемых ICANN; поддержка профессиональных услуг по разработке параметров

Поддержка политики по усилиям, связанным с БСО (политика)

Цели

Устанавливаются поддерживаемыми ОП и КК, ведущими деятельность в области БСО

- ОПРИ; ОПНИ
- ПКК
- ККСКС; РКК

Результаты

- Определяются на основе рабочих планов на 2011 ФГ по мере их утверждения

Ключевые заинтересованные стороны

- Названные ОП и КК
- Сотрудники отдела политик ICANN
- Сотрудники отдела безопасности ICANN

Ресурсы (2011 ФГ)

Кадровые —2 СПС

Финансовые — 550 тыс. долл. США на СПС и ограниченную дополнительную финансовую поддержку деятельности, связанной с БСО

Консультативный комитет по безопасности и стабильности (ККБС)

Цели

- Содействие развертыванию DNSSEC
- Обеспечение стабильности корневой зоны по мере ее роста и усложнения
- Защита регистрации доменов
- Сокращение масштабов злоупотреблений доменными именами
- Обеспечение стабильности системы адресов

Результаты

- Отчеты, рекомендации, комментарии
  - исследования масштабирования корневой зоны
  - исследование защиты доменных имен
  - исследование регистрационных данных: отображение, доступ, точность

Ключевые заинтересованные стороны

- Внешнее сообщество обеспечения безопасности Интернета
- Сообщество IANA и корневых серверов
- ОПРИ и ОПНИ
- РКК
- Организация поддержки адресов (ОПА)
- Сотрудники ICANN
- ПКК и Правление

Ресурсы (2011 ФГ)

Кадровые — 1,5 СПС

Финансовые — 650 тыс. долл. США на СПС и ограниченную дополнительную финансовую поддержку деятельности, связанной с командировками и публикациями; поддержку завершения исследований масштабирования корневой зоны

Приложение Б — Глоссарий терминов и сокращений, используемых в плане по БСО

ПРНЧП — планирование реагирования на нападения и чрезвычайные происшествия.

Дополнительный льготный период — пятидневный льготный период с момента регистрации регулируемого ICANN домена второго уровня. Владельцы регистрации имеют право отменить регистрацию в течение этих пяти дней, при этом регистрационный взнос полностью возмещается реестром доменных имен.

РГБФ — рабочая группа по вопросам борьбы с фишингом.

НАС — номера автономной системы. В рамках Интернета автономная система (АС) — это набор связанных префиксов IP-маршрутизации, представляющий единую, четко определенную политику маршрутизации в Интернете. Поставщики услуг Интернета (ISP) должны официально зарегистрировать номер автономной системы (НАС) в IANA.

ОПНИ — Организация поддержки национальных имен ICANN является органом разработки политики на глобальном уровне по узкому кругу вопросов, связанных с национальными доменами верхнего уровня, 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 национального 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.

FIRST — Форум групп быстрого реагирования и отделов безопасности.

рДВУ — родовой домен верхнего уровня.

IANA — Агентство по распределению номеров Интернета.

ИДИ — интернационализированное доменное имя.

IETF — Комиссия по технологиям Интернета.

IP — интернет-протокол определяет формат пакетов и схему адресации. В большинстве сетей IP сочетается с протоколом более высокого уровня под названием протокол управления передачей (TCP), устанавливающим виртуальную связь между точкой назначения и источником. По сути IP похож на почтовую систему. Он позволяет Вам адресовать 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 — четвертая версия интернет-протокола является четвертым поколением IP и первой версией, получившей широкое распространение. Вместе с IPv6 он составляет ядро основанных на стандартах методов межсетевого обмена в Интернете и до настоящего времени по-прежнему является наиболее широко распространенным протоколом межсетевого уровня.

IPv6 — шестая версия интернет-протокола является следующим поколением протокола межсетевого уровня для передачи данных с коммутацией пакетов между сетями и в Интернете. В декабре 1998 г. Комиссия по технологиям Интернета (IETF) выбрала IPv6 в качестве преемника версии 4, опубликовав спецификацию стандарта RFC 2460.

ISOC — Общество Интернета.

ИТ — информационная технология.

Бот-сети — чаще всего создаются обманным путем, заставляя обычных пользователей открывать на своих компьютерах приложения, которые на первый взгляд являются безвредными, но на самом деле устанавливают скрытое программное обеспечение, позже используемое для нападения. Зараженные компьютеры или «боты» соединяются в сети, которыми затем можно управлять по желанию, чаще всего для злонамеренных атак.

«Отравление» кэша — использование уязвимости в программном обеспечении системы DNS, чтобы заставить ее принять неверную информацию, из-за которой сервер затем заносит в кэш-память неверные данные и направляет все последующие запросы к серверу на новый домен с фальшивым подтверждением подлинности.

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.

Распределенная атака типа «отказ в обслуживании» (DDoS) — разновидность атаки типа «отказ в обслуживании», при которой нападающий используетзлонамеренный код, установленный на нескольких системах для нападения на единственную цель. Этот метод наносит больший вред цели, чем было бы возможно всего с одним атакующим компьютером. В Интернете распределенная атака типа «отказ в обслуживании» — это атака, при которой множество зараженных систем нападают на единственную 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. Коэффициент усиления по оценкам составляет около 1:73. Атаки, основанные на данном методе, достигали 7 Гигабит в секунду.

DNS — система доменных имен, которая осуществляет преобразование доменных имен (буквенных) в IP-адреса (цифровые). В целях простоты запоминания доменные имена представлены символами алфавита. 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 преобразует буквенное имя в соответствующий цифровой IP-адрес.

DNSSEC — расширения безопасности системы доменных имен обеспечивают способ подтверждения того, что данные системы доменных имен (DNS) не изменились во время передачи по Интернету. Это обеспечивается включением в иерархию DNS пар, состоящих из открытого и закрытого ключей подписи, для формирования цепочки доверия, создаваемой в корневой зоне. Важно отметить, что DNSSEC не является разновидностью шифрования. Эта технология обеспечивает обратную совместимость с существующей DNS; записи остаются в первоначальном виде — незашифрованными. Целостность записей обеспечивается в

DNSSEC при помощи цифровых подписей, подтверждающих подлинность записей.

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 передан для распространения в другую организацию (на данный момент в корпорацию VeriSign). Другими словами, организация, отвечающая за первичную основу доверия, — подтверждение изменений корневой зоны операторами доменов высшего уровня — должна также проверять правомочность конечного продукта до его распространения.

Опережающее использование доменных имен — сомнительная практика, используемая некоторыми регистраторами доменных имен, владеющими инсайдерской информацией и использующими ее для упреждающей регистрации доменных имен с намерением последующей спекулятивной продажи владельцам регистрации, 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 доменного имени на рынке. В течение указанного периода владельцем регистрации проводится анализ экономической эффективности и возможности получения дохода от размещения рекламных объявлений на веб-сайте этого домена.

Пробное использование домена не следует путать с **обманным использованием домена**, представляющим из себя механизм удаления доменного имени в течение пятидневного периода пробного использования и немедленной повторной регистрации еще на один пятидневный период. Этот процесс повторяется любое 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 серверов имен DNS, которые он использует, на «удобные для пользователей» имена, содержащиеся в фишинговых сообщениях, рассылаемых по электронной почте. В обоих случаях изменения происходят очень быстро (занимают порядка трех минут), что практически не оставляет экспертам времени на реагирование. ККБС ICANN тесно работает совместно с организациями по защите торговых марок и правоохранительными органами, а также с реестрами и регистраторами над выявлением мер противодействия, в особенности предотвращающих использование DNS в процессе «Fast Flux».

Fast Flux — техника ухода от обнаружения, применяемая фишерами, мошенниками, использующими чужие личные данные, и прочими лицами, совершающими электронные преступления, для противодействия усилиям групп реагирования и правоохранительных органов по отслеживанию и закрытию противозаконных веб-сайтов. Техника «Fast Flux» сильно напоминает игру в «наперсток», в которой мошенник кладет три согнутые карты на стол, а жертву обманом заставляют ставить на свое 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.

Зловредная программа (malware) — слияние слов «malicious» («зловредная») и «software» («программа») часто используется в качестве фразы, обозначающей компьютерные вирусы, червей, троянские программы, руткиты, шпионское ПО, рекламное ПО, преступное ПО и любое другое нежелательное программное обеспечение, установленное на компьютере пользователя с его согласия или без его ведома. Зловредная программа считается таковой, скорее, на основании воспринимаемого намерения его создателя, чем на основе каких-то конкретных характеристик программ.

ЦСО — центр сетевых операций является физическим местом, из которого обычно осуществляется управление, контроль и

надзор за крупной сетью. ЦСО также обеспечивают доступность сети для пользователей, подключающихся к ней извне этого физического пространства.

ГОС — группа операторов сетей.

ОНР — Организация номерных ресурсов.

Патчи — программы, предназначенные для устранения уязвимостей ПО; часто устанавливаются автоматически, чтобы сократить необходимость участия конечного пользователя и упростить использование.

Фишинг — форма интернет-мошенничества, направленная на кражу ценной информации, например номеров кредитных карт и социального страхования, пользовательских имен и паролей, путем 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 — соглашение об аккредитации регистраторов.

Реестр — организация, осуществляющая управление регистрацией доменных имен верхнего уровня Интернета.

Регистратор — компания, уполномоченная на регистрацию доменных имен Интернета.

РИР — региональный интернет-реестр.

ИОКР —инфраструктура открытых ключей ресурсов.

ПОУР — процесс оценки услуг реестра.

ГТОУР —группа технической оценки услуг реестра.

Спам — любые непрошенные сообщения электронной почты. Хотя обычно он рассматривается просто как дорогостоящий раздражитель, в наши дни спам часто содержит зловредное ПО. Зловредное ПО — это класс зловредных программ (вирусы, черви, трояны и шпионское ПО), целью которого является инфицировать компьютеры и системы для кражи важных сведений, удаления приложений, дисков и файлов или обращения компьютера в инструмент для постороннего лица или злоумышленника.

Спуфинг — вид нападения, при котором лицо или программа выдают себя за других путем 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, но вместо этого скрытно осуществляет зловредные функции, открывая недозволенный доступ к хост-машине, позволяя пользователям трояна сохранять свои файлы на компьютер ничего не подозревающего пользователя, или даже наблюдать за экраном пользователя и управлять его компьютером.

Вирус — программа или строка кода, которая загружается на компьютер без ведома пользователя и запускает зловредное программное обеспечение. Даже простейший вирус способен самовоспроизводиться, что делает его еще более вредоносным, так как он быстро использует всю доступнуюпамять инфицированной компьютерной системы.

Червь — схож с вирусом по природе; червь считается разновидностью вируса, но несет большую опасность по причине его способности самостоятельно распространяться в сети. Черви переносятся с компьютера на компьютер, но в отличие от вирусов, они способны перемещаться без какого-либо намеренного или случайного 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 ничего не подозревающего пользователя. Затем он размножается на инфицированных компьютерах и снова распространяется через записные книги электронной почты в новых инфицированных системах; он продолжает поглощать оперативную память, пока не займет столько памяти и пропускной способности, что это может привести к остановке работы целых сетей.