# ICANN — концепция обеспечения безопасности, стабильности и отказоустойчивости в *2012* финансовом году

*2 мая 2011 г.*

# Безопасность, стабильность и отказоустойчивость

*Часть Б — модуль 2012 ФГ*

# Компоненты новой концепции

Часть А

- Раздел, посвященный фундаментальным вопросам — миссия, основные ценности, подтверждение обязательств
- Экосистема и роль ICANN

Часть Б — модуль 2012 финансовый год

- Категория действий
- Стратегические проекты; работа с сообществом
- Организационные и управленческие области программы

# Три категории действий по обеспечению БСО

- Области деятельности ICANN
  - Среди прочего — внутренние вопросы ИТ, вопросы корневого сервера L, работа DNS, IANA, соответствие требованиям, оценка строк, логистика проведения конференций, управление и финансы
- Области, в которых ICANN занимается организацией, сотрудничеством и поддержкой работы сообщества
  - Координация в области разработки политики, поддержка секретариата, привлечение экспертов, участие в разработке протокола, сотрудничество с расширенным сообществом Интернета, в том числе с техническим сообществом
- Области, в которых ICANN выступает в роли наблюдателя или следит за действиями других сторон в экосистеме Интернета

| Области интереса | Программа/инициатива | Организационное руководство |
|---|---|---|
| Ответственность за операции | Функции IANA | Персонал, ответственный за функции IANA |
| | Работа DNS и корневого сервера L | Персонал, ответственный за работу DNS |
| | Управление DNSSEC | Персонал, ответственный за работу DNS |
| В т. ч. организационная поддержка ICANN, | ИТ и безопасность внутренних сетей | Персонал отдела безопасности ICANN и отдела ИТ |
| Финансы, кадры, юридическое обеспечение | Безопасность конференций | Персонал отдела безопасности ICANN |
| Административные задачи | Физическая безопасность и безопасность персонала | Персонал отдела безопасности ICANN |
| | План непрерывности деятельности ICANN и План связи в критических ситуациях | Персонал отдела безопасности ICANN и отдела ИТ |
| | Выполнение договорных обязательств | Персонал отдела соблюдения договорных обязательств |
| | Управление ускоренным вводом ДВУ с ИДИ | Отдел ИДИ |
| | Введение новых рДВУ | Отдел введения новых рДВУ |

| Области интереса | Программа/инициатива | Организационное руководство |
|---|---|---|
| Координация | Процесс разработки политики | ОП, КК + отдел политик |
| | Автоматизация управлением корневой зоной | Партнеры в управлении корневой зоной Управление по телекоммуникациям, ICANN, Verisign |
| | IPv6/IPv4 | ОНР, РИР, ICANN |
| Помощь | Поддержка секретариата для ОП и КК | Персонал отдела политик ICANN |
| | Техническая эволюция Whois | Сообщество + ICANN |
| Сотрудничество | Наращивание потенциала DNS | ICANN + Центр ресурсов для запуска сетей, региональные организации ДВУ, Общество Интернета, сообщество |
| | Разработка ИОКР | Работа DNS + ОНР, РИР |
| | Разработка протокола | Инженерная проектная группа Интернета (ИПГИ) |
| | Измерения и показатели DNS | RIPE, NCC, DNS-OARC, прочие |
| | Руководящие принципы ИДИ; управление вариантами ИДИ | Реестры + ICANN; сообщество |

| Области интереса | Программа/инициатива | Организационное руководство |
|---|---|---|
| Координация | Работа с операторами корневых серверов | ККСКС |
| Помощь | Всемирный симпозиум по БСО | Персонал отдела безопасности + сообщество |
| Участник | Показатели отказоустойчивости, надежная работа DNS | ENISA + CERT, другие |
| Координация | Принятие и развертывание DNSSEC. | Работа DNS + реестры, регистраторы и пользователи |
| Помощь | Совещания ОПНИ, технические конференции | Сообщество нДВУ |
| Сотрудничество | Стратегия управления рисками DNS | Усилия сообщества получают поддержку отдела безопасности |
| Помощь | Рабочая группа по вопросам анализа безопасности и стабильности DNS | Участники ОП и КК с независимыми экспертами |
| Сотрудничество | Глобальная разъяснительная работа в сфере безопасности, привлечение к работе и повышение осведомленности | Отдел безопасности ICANN и Отдел глобального сотрудничества |
| Сотрудничество | Взаимодействие с сообществом безопасности на основе доверия, бизнесом и правоохранительными органами | Персонал отдела безопасности ICANN |

| Области интереса | Программа/инициатива | Организационное руководство |
|---|---|---|
| Осведомленность о деятельности | Деятельность ИПГИ и IAB | ИПГИ, IAB |
| других в сообществе; | Деятельность ОНР и РИР | AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC |
| Роль наблюдателя | Деятельность региональных организаций ДВУ | AfTLD, APTLD, CENTR, LACTLD |
| | Международные учения по деятельности в киберпространстве (в некоторых случаях участие) | Координация учений (DHS, ENISA, другие) |
| | Правительственные программы по борьбе с киберпреступностью и защите ключевой инфраструктуры | Правительства, IT-SCC, другие |
| | Надежная идентификация в киберпространстве | |
| | Инициативы правоохранительных органов в отношении злонамеренных действий | Interpol, международные организации правоохранительных органов |
| | Инициативы по управлению рисками | |
| | Научные исследования DNS | |
| | Развитие практики регистрации | Реестры, регистраторы, сообщество |

# Стратегические цели на 2011-14 гг.

1. Поддержка и осуществление безотказного функционирования DNS
2. Повышение безопасности системы уникальных идентификаторов в целом
3. Расширение международного участия в обеспечении безопасности системы уникальных идентификаторов
4. Координирование глобального управления рисками DNS

# Работа с сообществом

- Внедрение и распространение DNSSEC на локальном уровне
- Интернационализированные регистрационные данные Whois
- Разработка решений для обеспечения безопасности DNS (и системы уникальных идентификаторов) — РГ по вопросам анализа безопасности и стабильности DNS и пр.
- Развертывание IPv6; управление рисками, связанными с истощением диапазона IPv4
- Развертывание инфраструктуры открытых ключей ресурсов (ИОКР) — с региональными реестрами
- Ситуационные исследования вариантных ИДИ

# Ключевые области работы отдела безопасности

- Глобальная разъяснительная работа в сфере безопасности (вовлечение, осведомленность мирового сообщества и более широкого сообщества ICANN)
- Сотрудничество в области безопасности
- Наращивание потенциала DNS
- Программы корпоративной безопасности (в т. ч. информационная безопасность ICANN, безопасность во время проведения конференций, личная безопасность сотрудников), непрерывность бизнеса, управление рисками
- Общеорганизационная поддержка (в т. ч. рДВУ, ИДИ, DNSSEC, разработка политики, соответствие требованиям, глобальные партнерские отношения и отношения с правительствами)

# Операции по обеспечению БСО в 2011-2014 ФГ

| Разъяснительная работа по глобальной безопасности | Деятельность и мероприятия в 2012 г. |
|---|---|
| Участие в работе расширенного сообщества, бизнеса, научного и технического сообществ и правоохранительных органов | Симпозиум по БСО DNS — ориентировочно в Европе в 3 квартале 2011 г. или в 1 квартале 2012 г. |
| | Участие в мероприятиях с региональными партнерами |

| Сотрудничество | |
|---|---|
| Поддержка принятия средств измерения и учета показателей работы DNS, таких как программа ATLAS реестра RIPE NCC | Помощь и поддержка размещения узлов в пограничных зонах сети для проведения измерений и анализа данных |
| Автоматизация корневой зоной | Внедрение систем автоматизации совместно с NTIA и Verisign |
| Развертывание и принятие DNSSEC | Поддержка обучения и способствование принятия развивающимися ДВУ, регистраторами и пользователями |
| Разработка механизмов сертификации ресурсов/ ИОКР | Работа с РИР |

# Операции по обеспечению БСО в 2011-2014 ФГ

| Сотрудничество | Деятельность и мероприятия в 2012 г. |
|---|---|
| Рабочая группа по вопросам анализа безопасности и стабильности DNS проводит оценку рисков, угроз и недостатков в механизмах защиты DNS | Рабочая группа следует утвержденному графику, результаты ее работы могут быть опубликованы в 2012 ФГ |
| Техническая эволюция Whois | Поддержка усилий других в 2012 ФГ |
| Разработка политики — злоупотребления при регистрации; Соглашение об аккредитации регистраторов | Поддержка деятельности ОПРИ и ОПНИ в области разработки политики |
| DNSSEC — периодическая смена ключей и аудит | Полный аудит SysTrust и успешное проведение церемонии KSK при смене ключей |

| Программы корпоративной безопасности | |
|---|---|
| Повышение безопасности внутренних сетей ICANN, управления доступом и процессов в соответствии с передовыми практическими методами согласно ISO 27002 | Реализация улучшения процессов путем оценки уязвимостей и тестирования; оптимизация ресурсов и подготовки персонала |
| Отказоустойчивость зоны корневого сервера L | Внедрение улучшений, определенных в результате учений по обеспечению непрерывности работы сервера корневой зоны L в 2011 г.; отдельные узлы корневой зоны L |

# Операции по обеспечению БСО в 2011-2014 ФГ

| Программы корпоративной безопасности | Деятельность и мероприятия в 2012 г. |
|---|---|
| Повышение подготовки персонала в поддержку оптимизации практики работы внутренней группы ICANN по быстрому реагированию на происшествия в сфере компьютерной безопасности | Обучение персонала отделов ИТ и безопасности по программе SANS или аналогичной |
| План непрерывности деятельности в Интернете и учения по связи в кризисной обстановке | Оставить сотрудников на полной занятости для поддержания непрерывности работы и поддержки учений |
| Безопасность конференций — оценка рисков и местоположения, безопасность гостей | Оценка рисков по местам проведения собраний ICANN в 2012 ФГ; наземная безопасность, безопасность гостей и аварийный службы |

| В масштабах всей организации | |
|---|---|
| Введение новых рДВУ | Запуск процесса новых рДВУ (после утверждения программы); проверка уязвимости системы TAS; [см. отдельный слайд о новых рДВУ] |
| Выполнение договорных обязательств | Расширение штата на 3 или более сотрудников; обеспечение выполнения обязательств реестрами и регистраторами |

# Операции по обеспечению БСО в 2011-2014 ФГ

| В масштабах всей организации | Деятельность и мероприятия в 2012 г. |
|---|---|
| Поддержка программы ИДИ | Поддержка процессов проверки строк, Комиссия по стабильности DNS; выпуск информационных материалов по ИДИ и практическим методам обеспечения безопасности; ситуационные исследования управления вариантными ИДИ |
| Управление корпоративными рисками | Поддержка внутренних процессов управления рисками, в том числе комитета Правления по вопросам рисков; проведение повторной оценки рисков до принятия Плана работ и бюджета на 2013 год |
| Поддержка отдела глобальных партнерских отношений и отношений с правительствами | Помощь по информационной поддержке и разъяснению того, как требования правительств могут влиять на систему уникальных идентификаторов Интернета; поддержка сотрудничества с партнерами и заинтересованными сторонами |

# Работа с сообществом по обеспечению БСО

- Улучшения Соглашения об аккредитации регистраторов — ОПРИ
- Операции ККБС и ККСКС
- Совместное реагирование на злонамеренные действия в отношении системы уникальных идентификаторов — червь Conficker и сообщество безопасности на основе доверия
- Разработка политик, например, рабочая группа по вопросам злоупотреблений при регистрации; интернационализированные данные Whois

# Отслеживание ключевых областей, относящихся к документу Подтверждение обязательств

- Продолжающаяся и незапланированная работа
- Поддержка четкости процессов
- Уделение особого внимания возникающим угрозам и рискам

# Продолжающаяся и незапланированная работа

- Программа по наращиванию потенциала DNS, в том числе реагирование на нападения и чрезвычайные происшествия, Курсы по стабильной работе реестров для региональных организаций и операторов ДВУ, обучение и поддержка по вопросам DNSSEC
- Планы и учения ICANN по реагированию на чрезвычайные происшествия
- Участие в международных учениях вместе с операторами
- Процессы ответственного хранения данных и программа ответственного хранения данных регистраторов

# Программа по наращиванию потенциала DNS

- Проведение обучения в партнерстве с Центром ресурсов для запуска сетей, ISOC и региональными организациями ДВУ (AfTLD, APTLD, LACTLD)
- За период работы данной программы в ней приняли участие свыше 250 представителей от нДВУ из развивающихся регионов
- В 2010/11 гг. обучение проводилось в Мали, Иордании, Гватемале, Гонконге (поддержка мероприятий в Никарагуа и Кении перед конференцией ICANN в Сингапуре)
- На 2012 ФГ запланировано по меньшей мере 8 учебных семинаров, которые будут проводиться по очереди в регионах Африки, Латинской Америки и Азии

# Поддержка четкости процессов

- Группа технической оценки услуг реестра — ГТОУР
- Комиссия по стабильности DNS в программе ускоренного ввода нДВУ с ИДИ
- Оценка похожести и конфликтности строк в процедуре ускоренного ввода нДВУ с ИДИ
- Программа новых рДВУ
- Техническая эволюция Whois
- Управление корпоративными рисками

# Возникающие угрозы и риски

- Угрозы злоупотребления DNS и системой уникальных идентификаторов
  - Бот-сети
  - DoS-атаки
  - Социальная техника, мошенничество, злонамеренное поведение
  - Перехват маршрутов
- Угрозы фундаментальной инфраструктуре
  - Неспособность регистраторов выполнять свои обязательства в отношении ДВУ
  - Стихийные бедствия
  - Нарушения авторизации и проверки подлинности

# Возникающие проблемы

- Внедрение ИДИ и прием заявок, проблемы, связанные с вариативностью, таблицы ИДИ
- Вмешательство правительств
- Внедрение и принятие DNSSEC
- Проблемы пространства адресов IPv6/IPv4 — работа с РИР
- Взаимодействие между DNS и приложениями (мобильными приложениями, социальными сетями и т. п.) — в поддержку осведомленности
- Расширение привлечения к обеспечению БСО правоохранительных органов и сообщества пользователей

# Работа с возникающими угрозами

- Рабочая группа по вопросам анализа безопасности и стабильности DNS
  - Устав, утвержденный на конференции в Картахене в декабре 2010 г.
  - Рабочая группа в составе представителей РКК, ОПНИ, ОПРИ, ОНР, ПКК, ККБС и прочих специалистов
  - При участии и под руководством представителей сообщества
    1. РГ рассмотрит фактический уровень, частоту и серьезность угроз в отношении DNS
    2. Текущие усилия и действия, направленные на снижение подобных угроз
    3. Бреши, если таковые имеются, в текущем реагировании систем безопасности на проблемы DNS

# Текущая работа в области совместного реагирования

- Совместное реагирование на бот-сети и злонамеренное поведение — ICANN продолжит участие в работе рабочей группы по борьбе с Conficker и сотрудничество в этом направлении с сообществом безопасности на основе доверия, поставщиками услуг реестров и правоохранительными органами на благо всего сообщества Интернета
- Поддержка усилий рабочих групп по борьбе с фишингом и злоупотреблениями в области рассылки сообщений; сотрудничество с Центром анализа и обмена информацией в области ИТ (IT-ISAC)

# Выделение ресурсов в 2012 ФГ

- В проектах Операционного плана и бюджета ICANN на 2012 ФГ запланированы расходы на сумму 69,8 млн. дол. США
- Доля расходов на инициативы по обеспечению БСО в целом оценивается на уровне 17% от всего бюджета ICANN (приблиз. 12 млн. дол. США в 2012 ФГ)

# Заключение

План ICANN по обеспечению безопасности, стабильности и отказоустойчивости "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".

Настоящая концепция призвана продемонстрировать развитие стратегического и операционного планирования ICANN в вопросах обеспечения безопасности, стабильности и отказоустойчивости, а также признание ограниченности возможностей ICANN и стремление к сотрудничеству на благо всего сообщества.

Один мир

Один Интернет

# Дополнительная информация: icann.org/en/security