Предлагаемые инициативы в области совершенствования безопасности, стабильности и отказоустойчивости DNS

Представлено

Корпорацией Интернета по распределению имён и адресов (ICANN)

Для общественного обсуждения

12 февраля 2010 г.

Предлагаемые инициативы в области совершенствования безопасности, стабильности и отказоустойчивости DNS

1. Обзор

В настоящем документе излагается обоснование, основные характеристики и прогнозируемые расходы двух стратегических инициатив, связанных с безопасностью, стабильностью и отказоустойчивостью системы доменных имён (DNS), которые, по мнению ICANN, являются необходимыми для выполнения её обязательств в соответствии с Уставом, подтверждение обязательств от 2009 г. и стратегическим планом ICANN на 2010-2013 годы. Настоящий документ обеспечивает основу для многостороннего обсуждения предлагаемых инициатив, обязанностей ICANN по формированию предлагаемых мощностей и способов организации усилий общественности по поддержке данных инициатив. Выявлена потребность в значительных кадровых и материальных ресурсах, но возможные альтернативы финансирования данных инициатив не анализируются.

Примечание: Данные инициативы предлагаются в качестве дополнительных мер к описанным в структуре плана работ и бюджета ICANN на 2011 финансовый год, опубликованном для обсуждения на конференции в Найроби.

2. Предположения

2.1 Система доменных имён стала одной из основополагающих, базовых служб, поддерживающих работу Интернета. DNS обеспечивает пользователей Интернета возможностью поиска имён, а также лежит в основе служб электронной почты, обмена текстовыми сообщениями, голосовой связи через Интернет и прочих ключевых служб и протоколов Интернета. В то же время, DNS существует в условиях возрастающих угроз и рисков. С технической точки зрения деятельность системы подвержена целому ряду воздействий, таких как распределённые атаки типа "отказ в обслуживании" (DDoS) на авторитетные серверы имён и распознаватели на уровнях вплоть до корневых серверов имён, атаки с "отравлением" кеша, влияющие на целостность системы поиска имён в DNS, описанные исследователем в области безопасности Дэном Камински (Dan Kaminsky), и прочие методы, включая социально-технические нападения, позволяющие неправильно адресовать и злоупотреблять услугами DNS. Кроме того злоумышленники и преступники пользуются зависимостью пользователей от DNS и используют систему различными способами для осуществления самых разнообразных видов вредоносной деятельности.

2.2 В настоящее время сообщество операторов, предоставляющих услуги DNS, активно сотрудничает с поставщиками, исследователями в области безопасности, правоохранительными органами и группами реагирования с целью противодействия возникающим угрозам, но осуществляется оно несистемно. В рамках сообщества DNS существуют инициативы по улучшению обмена

информацией, выявлению вредоносной деятельности и расширению сотрудничества, связанные с DDoS и прочими общесистемными нападениями. Эти совместные усилия, как правило, сопряжены с добровольной совместной работой DNS и участников сообщества обеспечения безопасности по решению возникающих ситуаций. В прошлом году прозвучал ряд призывов к действиям по ликвидации и уменьшению системных рисков для DNS.[1] Частота и серьёзность характер этих призывов к действию указывают на растущую потребность в общесистемной оценке рисков, планировании на случай чрезвычайных ситуаций и механизмов немедленного реагирования.

2.3 Текущие усилия, направленные на борьбу с различными угрозами и рисками для DNS, несистемны и нецеленаправленны. На оперативном уровне обеспеченные необходимыми ресурсами искушённые в вопросах безопасности операторы DNS разработали надёжные механизмы для понимания угроз и принятия мер по уменьшению рисков для себя и своих клиентов. Однако сотрудничество в этой области, как правило, не распространяется на менее способных и хуже финансируемых операторов DNS и прочие заинтересованные стороны, не осведомлённые об угрозах и рисках и не имеющие возможности адекватно реагировать при возникновении таких угроз для безопасности, стабильности и отказоустойчивости. Кроме того, приложенные ранее усилия показали, что для борьбы с угрозами, не поддающимися воздействию легко локализуемых технических решений, необходима постоянная сосредоточенность на контроле, реагировании и восстановительных работах. На более высоком уровне DNS недостаёт общесистемных точек приложения внимания в плане подотчётности, связанной с ключевыми мощностями в области оценки рисков, планирования на случай чрезвычайных ситуаций и учебных мероприятий, и целенаправленных, устойчивых средств реагирования. Эти виды деятельность должны сочетаться с целостным подходом к DNS и реагировать на потребности её отдельных компонентов и операторов.

2.4 Такие виды мощностей по сути своей не могут полностью полагаться на усилия добровольцев, действующих без целенаправленной организационной поддержки, проработанных оперативных подходов и долгосрочного обеспечения ресурсами. Усилия, направленные на обеспечение стабильности и устойчивости DNS, должны достичь уровней эффективности и подотчётности, соответствующих прочим ключевым аспектам коммуникационной инфраструктуры, требующим схожих инвестиций в плане занятых на постоянной основе сотрудников и поддержки.

[1] См. http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips, http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks и http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf.

3. Роль и обязанности ICANN

3.1 DNS должна работать безопасно, стабильно и устойчиво. На ICANN возложен ряд обязательств, требующих приложения усилий для достижения этой цели. В статье I Устава ICANN говорится: "Задача ICANN заключается в координации на общем уровне глобальных систем уникальных идентификаторов Интернета, и, в частности, в обеспечении стабильности и безопасности деятельности систем уникальных идентификаторов Интернета". В подтверждении обязательств от 2009 года (http://icann.org/en/announcements/announcement-30sep09-en.htm) говорится, что DNS выполняет важнейшую роль в экосистеме Интернета, и, следовательно, требуется надлежащее управление рисками, связанными с деятельностью. ICANN взяла на себя обязательство "поддерживать безопасность, стабильность и устойчивость DNS". Кроме того, в подтверждении от ICANN требуется выявлять существующие и будущие угрозы и осуществлять соответствующее планирование на случай чрезвычайных ситуаций.

3.2 Смысл этих обязательств для ICANN ясен. В подтверждение обязательств от ICANN требуется предпринимать совместные усилия для выявления и уменьшения рисков для безопасности и отказоустойчивости в рамках распределённой системы DNS, включающей в себя широкий круг заинтересованных субъектов, предоставляющих и использующих услуги DNS.[2] Ввиду значимости DNS надёжное, устойчивое функционирование системы корневых серверов и доменов верхнего уровня должно быть важнейшим приоритетом для ICANN. Расширение DNS благодаря естественному приросту пользователей, внедрению новых технологий и предложениям по созданию новых ДВУ (в том числе с использованием интернационализированных доменных имён) требует от ICANN понимания и стремления к снижению рисков, которым подвержена система. Важно отметить, что с момента своего создания ICANN стремится повышать безопасность, стабильность и отказоустойчивость DNS. В плане ICANN по *повышению безопасности, стабильности и отказоустойчивости Интернета* (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) рассматривается широкий круг существующих программ и мероприятий. Инициативы, изложенные в данном документе, относятся к дальнейшим усилиям, которые должна прикладывать ICANN для выполнения этих обязательств.

3.3 Для улучшения системного понимания и уменьшения рисков DNS и выполнения взятых на себя обязательств от ICANN в сотрудничестве с сообществом DNS потребуется приступить к дальнейшей работе, основывающейся как на уже приложенных усилиях, так и на текущей совместной деятельности. С этой целью в стратегическом плане ICANN на 2010-2013 годы повышение стабильности, безопасности и отказоустойчивости DNS определено, как одно из четырёх

[2] Планируя пересмотр своей роли в управлении рисками для безопасности, стабильности и отказоустойчивости DNS, ICANN не затрагивает вопросы, связанные с национальной безопасностью, конкуренцией между государствами в области кибервойны и шпионажа, и не затрагивает контроль за содержанием, размещаемым в Интернете, затрагиваемые в плане ICANN по повышению безопасности, стабильности и отказоустойчивости Интернета. См. http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf.

основных направлений работы ICANN на указанный период. В частности, в стратегическом плане рассматривается требование к ICANN о разработке методики использования групп быстрого реагирования на нарушения компьютерной безопасности (CERT) для системы доменных имён (DNS-CERT), а также о планировании на случай чрезвычайных обстоятельств и о проведении учебных проверок для DNS. ICANN стремится прогрессировать, обеспечивая создание общесистемного подхода к оценке рисков, планирование на случай чрезвычайных обстоятельств и проведение учебных проверок по борьбе с потенциальными угрозами и организации совместных сил реагирования на инциденты для повышения общей безопасности, стабильности и отказоустойчивости системы DNS. ICANN также планирует предпринять усилия для улучшения общесистемных показателей, чтобы сообщество DNS можно получить более чёткое представление о безопасности, стабильности и отказоустойчивости DNS, предвидеть трудности и эффективно на них реагировать.

3.4 Достижение максимальной пользы и операционного успеха инициатив, изложенных ниже, требует общественной поддержки и участия. Анализ со стороны сообщества, обратная связь и планирование, связанные с реализацией данных инициатив будут интегрированы в процессы оперативного планирования и составления бюджета ICANN.

4. Риски для функционирования DNS

4.1 С началом 2010 год экосистема Интернета продолжает полниться энергией. Активность в Интернете всё больше и больше отражает полный спектр человеческой мотивации и поведения. Отчасти такая деятельность отражает открытую природу Интернета, принёсшую ему успех, позволяет осуществлять передовые нововведения и способствует общению, творчеству и торговле в глобальной среде. Этой экосистеме также угрожают увеличивающиеся уровни вредоносной деятельности, осуществляемой различными лицами, при наличии значительных признаков быстрорастущего участия преступных организаций. Среди наблюдаемых угроз можно перечислить мошенничество, вымогательство и прочие виды незаконной деятельности онлайн, подрывающие доверие пользователей к Интернет-услугам, а также атаки типа "отказ в обслуживании" (DoS) и другие деструктивные действия, дестабилизирующие инфраструктуру Интернета. В частности, способность злоумышленников посягать на функционирование самой DNS, равно как и лёгкость и частота, с которой они используют службы поиска имён и регистрации для осуществления вредоносной и преступной деятельности, представляют растущую опасность для нормальной работы Интернета и ставят под вопрос целостность и надёжность Интернета в качестве глобальной коммуникационной платформы.

4.2 Существует три основные категории рисков для безопасности, стабильности и устойчивости: вредоносная деятельность (нападения на DNS или нападения с эксплуатацией систем поиска имён и регистрации), технические риски для стабильности DNS и организационные риски, связанные с DNS.

4.2.1 Риски вредоносной деятельности

4.2.1.1 По сути, основной источник риска, представляющий интерес для ICANN, заключается в готовности DNS для поиска имён и обеспечения широкого ряда взаимодействий в Интернете. Серьёзную угрозу готовности могут представлять атаки DoS против операционных служб DNS на различных уровнях системы. Последствия атак DoS зависят как от типа подверженных нападению служб, так и от сложности атаки и объёма трафика, используемого в ней. За последние десять лет непосредственному нападению подвергалась деятельность, как корневых серверов, так и доменов верхнего уровня (ДВУ). Особого внимания заслуживают четыре случая. 1) 21 октября 2002 г. произошёл первый задокументированный случай координированного нападения на тринадцать корневых серверов DNS (http://d.root-servers.org/october21.txt); 2) в феврале 2006 года произошли нападения на серверы имён, управляемые одним из крупнейших поставщиков услуг ДВУ (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf); 3) в феврале 2007 года было совершено нападение на шесть из тринадцати корневых серверов DNS (http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf); 4) Совсем недавно, в декабре 2009 года, атаки типа DoS против поставщиков услуг DNS снова оказались в новостях, после того как нападение на службу UltraDNS фирмы NeuStar сказалось на многих сайтах электронной торговли (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html). История нападений свидетельствует о постоянном росте ресурсов, которыми располагают злоумышленники, а также об их изощрённости.

4.2.1.2 Прилагаются значительные усилия для снижения этих рисков, в частности, путём предоставления пропускной способности для продолжения работы при борьбе с DDoS, а также путём разработки и воплощения в жизнь технологий и методологий, таких, как резервирование (anycasting), при котором данные направляются в лучший или ближайший пункт назначения. Примером развёртывания решений с использованием резервирования является рост системы корневых серверов DNS с тринадцати объектов (систем) до более чем двухсот (дополнительная информация по адресу http://www.root-servers-org). Также растёт интенсивность планирования и сотрудничества между операторами DNS при создании таких организаций, как Центр анализа и исследований работы DNS (DNS-OARC) (http://www.dns-oarc.org), Группа безопасности Интернет-реестров (RISG) (http://registrysafety.org/website/), и развитии усилий по пониманию связанных с DNS рисков, таких, как глобальный симпозиум по безопасности, стабильности и отказоустойчивости DNS (http://www.gtisc.gatech.edu/pdf / DNS_SSR_Symposium_Summary_Report.pdf). Однако, возрастают и угрозы: как никогда крупные бот-сети, находящиеся под контролем преступных субъектов и прочих злоумышленников, представляют риск очень серьёзных с точки зрения сложности и масштаба нападений. При планировании мер на случай таких нарушений необходимо также учитывать возможность нарушения служб DNS в результате злонамеренных атак против систем, на которые полагается DNS, от обеспечения электроэнергией до Интернет-маршрутизации.

4.2.1.3 Открытость и распределённость DNS в сочетании с широко распределённым управлением серверами имён и распознавателями подвергают пользователей целому ряду дополнительных рисков. Протокол DNS (без использования расширений безопасности) уязвим для атак с использованием *ложного направления* запросов. В частности, в ходе нападения в ответ на запрос DNS предоставляется ложная информация (*отравление* или *фарминг*) либо информация, отличающаяся от предусмотренной компетентным органом доменного имени (переадресация или модификация ответа). Такие нападения на DNS нацелены на обман пользователей самым широким рядом способов: направление пользователей на веб-сайты с мошенническим содержанием или вредоносным кодом, придание электронной почте видимости происхождения из поддельных источников и так далее. Методы проведения атак, позволяющих систематическое отравление кеша DNS и, следовательно, неправильное направление Интернет-трафика, обеспечивают возможность для вредоносных действий, способных представлять опасность для целостности всей DNS.

4.2.1.4 Услуги регистрации доменных имён являются ещё одним вектором для атак злоумышленников. Нападающие используют технические (уязвимость веб-сайта) или оперативные слабости регистратора или владельца регистрации доменного имени (персонал, на который можно оказывать психологическое воздействие) для получения несанкционированного контроля над регистрационной учётной записью доменного имени (дополнительные сведения в SAC040 http://www.icann.org/en/committees/security/sac040.pdf). После установления контроля над захваченной регистрационной учётной записью злоумышленник изменяет конфигурацию DNS вплоть до всех доменов на захваченной записи так, чтобы они указывали на имя контролируемого им сервера, что обеспечивает злоумышленнику контроль над поиском адресов веб-страниц, электронной почты и прочих Интернет-приложений для выбранного домена. Такие атаки, направленные на похищение доменного имени или учётной записи, используются для искажения содержания веб-сайтов, нарушения служб электронной почты и прочих служб, предоставляемых владельцем регистрации, или для сбора конфиденциальной или личной информации.

4.2.1.5 Хотя DNS предназначена для обслуживания пользователей Интернета, к сожалению, её также используют злоумышленники в целях осуществления широкого круга преступных деяний и злоупотреблений. Наилучшим примером этого непреднамеренного последствия является то, каким образом DNS эксплуатируется для способствования вредоносной деятельности, обычно называемой *фишингом*. Фишеры специально регистрируют доменные имена для поддержки нападений, осуществляемых из сетей взломанных или заражённых *ботами* компьютеров, называемых *бот-сетями*. Злоумышленники зачастую используют некоторые из этих вредоносных доменных имён для управления *преступной DNS*, представляющей собой набор распознавателей DNS, специально запрограммированных и направленных на обработку запросов в DNS, подаваемых жертвами фишинга. Другие вредоносные доменные имена используются для

размещения поддельных веб-сайтов. Ответы на запросы жертвы в DNS относительно, казалось бы, настоящего доменного имени финансового учреждения, электронного предприятия, благотворительной организации, государственного учреждения или подобного лица направляют ни о чём не подозревающих пользователей на обманные или поддельные сайты. Невинная жертва взаимодействует с обманным сайтом так же, как и при нормальном взаимодействии с настоящими сайтами финансовых учреждений, электронных предприятий, благотворительных организаций или государственных учреждений. Однако, эти вредоносные сайты предназначены для кражи личности, информации о банковских счетах и кредитных картах, продажи незаконной или поддельной продукции жертве, обмана благотворительных организаций и многого другого. [3]

4.2.1.6 DNS всё чаще играет видную роль в обеспечении существования *предлагаемых в наём ударных бот-сетей* на процветающем теневом рынке. Бот-сети состоят из сотен тысяч или даже миллионов заражённых компьютеров (ботов), управляемых дистанционно с целью осуществления многих типов вредоносных атак (например, DDoS) или поддержки преступной деятельности (торговли людьми, распространения незаконных фармацевтических препаратов, рассылки спама и т.д.). Для эффективного управления ботами с высокой степенью противодействия контрмерам, предпринимаемым предприятиями в области безопасности и сотрудниками правоохранительных органов, злоумышленники программируют ботов на использование DNS для определения адресов *точек встречи* или командования и управления, из которых команды высылаются ботам. В последнее время некоторые вредоносные программы, такие как варианты вредоносного ПО Conficker, используют подходы, стремящиеся опираться на наборы заранее определённых доменных имён, как один из ключевых аспектов управления ботами.

4.2.2 Технические риски

4.2.2.1 На деятельность и целостность DNS может быть оказано негативное воздействие, если широкое использование сомнительных методов работы приведёт к перебоям в предоставлении услуг, или если техническое изменение приведёт к возникновению непредвиденной уязвимости, используемой злоумышленниками или преступниками для облегчения вредоносной деятельности. Проблемы последнего рода и в значительной степени реактивные способы решения таких проблем, существующие на данный момент, обсуждались в 2008 году. Эксперт по вопросам безопасности Даниэль Камински (Daniel Kaminsky) обнаружил серьёзную уязвимость в протоколе DNS, а затем публично продемонстрировал, что злоумышленники могут использовать практику под названием изменение ответа DNS для похищения веб-сайтов крупнейших корпораций при помощи услуг веб-хостинга, находящихся абсолютно вне административной досягаемости данных

[3] Министерство национальной безопасности США, Координационный совет правительства по информационным технологиям. 2009 г. Базовая оценка рисков в секторе информационных технологий. Вашингтон, Колумбия, печатный офис правительства, стр. 32-33.

организаций. Консультативный комитет по безопасности и стабильности ICANN (ККБС) позднее опубликовал консультативное предупреждение о потенциальной угрозе, которую изменения ответа DNS создают для сообщества (http://www.icann.org/en/committees/security/ sac032.pdf). Были созданы временные системы, позволяющие операторам и пользователям DNS проверять свои системы на уязвимость и принимать превентивные меры или меры по исправлению положения. Сообщество ICANN уже инициировало и продолжает ряд инициатив, которые могут способствовать более координированному раскрытию и более организованной реакции на связанные с DNS угрозы такого рода. Среди них работа ICANN с партнёрами по проведению ежегодных симпозиумов, на которых встречающиеся эксперты изучают картину существующих угроз, совместно оценивают риски и выносят рекомендации относительно способов борьбы с ними. Первый симпозиум был проведён в феврале 2009 года совместно с центром информационной *безопасности* Технологического института Джорджии (GTISC).

4.2.2.2 На функционировании DNS также может отрицательно сказаться, если технические изменения в DNS приведут к изменениям в поведении системы или к возникновению нагрузок трафика, требующих внесения существенных изменений в текущие и планируемые мощности. Для сокращения потенциала принятия оперативных методов, способных подорвать безопасность и стабильность DNS на уровне ДВУ, в 2009 году Правление ICANN осуществило ряд мер по запрещению использования переадресации на основе рисков, которые создаёт эта практика для стабильности DNS, определённых консультативным комитетом по безопасности и стабильности (SAC041 http://www.icann.org/en/committees/security/sac041.pdf).[4] В 2010 году сообщество DNS продолжит всеобъемлющий анализ возможных последствий, вытекающих из ряда изменений, которые предлагается внести на корневом уровне DNS: внедрения расширений безопасности DNS (DNSSEC), реализации протокола IPv6 и необходимости добавления для "клейких" записей IPv6 в файл корневой зоны, введение ускоренного режима, позволяющего использовать интернационализированные доменные имена (ИДИ) на верхнем уровне DNS, а также ввод новых рДВУ.

4.2.3 Сбои в работе организаций

4.2.3.1 Возможные сбои в эффективной деятельности организаций, выполняющих ключевые функции в работе DNS, также представляют собой значительную категорию риска. Лежащая в основе DNS способность ICANN, операторов корневых серверов, реестров и регистраторов ДВУ предоставлять свои услуги бесперебойно имеет важное значение для общей безопасности и стабильности DNS. Каждая из этих организаций несёт отдельную ответственность за свою собственную финансовую устойчивость, непрерывность деятельности и управление рисками, но на системном уровне необходимо предусмотреть чрезвычайные обстоятельства,

[4] Министерство национальной безопасности США, Координационный совет правительства по информационным технологиям. 2009 г. Базовая оценка рисков в секторе информационных технологий. Вашингтон, Колумбия, печатный офис правительства, стр. 32-33.

при которых та или иная организация больше не сможет должным образом выполнять свою функцию, и то, каким образом будут восстановлены, сохранены или преобразованы её услуги в обеспечение дальнейшей эффективной работы DNS и защиты владельцев регистраций.

4.2.4. Измерение рисков для безопасности, стабильности и отказоустойчивости

4.2.4.1 В настоящее время не существует согласия по правильным мерам и приемлемому уровню показателей системы в целом в отношении рисков для безопасности, стабильности и отказоустойчивости. Индивидуальные операторы и независимые исследователи измерили различные аспекты DNS, но на сегодняшний день был достигнут лишь незначительный прогресс в определении и реализации стандартных общесистемных показателей или приемлемого уровня обслуживания. Усилия, направленные на улучшение управления рисками, связанными с безопасностью, стабильностью и отказоустойчивостью DNS, должны руководствоваться повышением способности измерять эти характеристики и оценивать полезность программ и вложений ресурсов.

4.2.4.2 Ключевым фактором, который позволит улучшить ситуацию, станет обеспечение правильной подготовки и измерения составных частей операций DNS. В отчёте комитета по исследованию корневых серверов (КИКС) за 2009 г. о масштабировании корневой зоны (http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf) содержится призыв к "созданию эффективных механизмов для выявления и уменьшения рисков, по мере того, как они становятся видимыми", связанных с системой корневых серверов. В ходе установления показателей и подготовки приборов возникают некоторые интересные задачи. В частности, распределённый характер DNS требует кооперативной модели измерения, в которой должно принимать участие несколько участников и организаций. Тема систем раннего предупреждения для Интернета в настоящее время изучается на различных форумах, в том в числе в Европейском агентстве по сетевой и информационной безопасности (ENISA), проводящем свой первый семинар по системам раннего предупреждения и сбору сетевой информации в Интернете в марте 2010 г. (http://www.enisa.europa.eu/events/ee/ EWNI2010). В сотрудничестве с университетом Киото ICANN провела второй глобальный симпозиум по безопасности, стабильности и отказоустойчивости DNS в феврале 2010 года, с особым упором на измерение. ICANN планирует поощрять и принимать участие в деятельности, позволяющей улучшить понимания того, как следует измерять риски DNS для здоровья, безопасности, стабильности и отказоустойчивости системы в роли ключевого катализатора эффективной оценки рисков, планирования и учений на случай чрезвычайных обстоятельств и мощностей реагирования.

5. Стратегические инициативы

5.1 Две представленные здесь инициативы отвечают важнейшим потребностям по созданию потенциала, необходимого ICANN для выполнения данных ранее обязательств по безопасности, стабильности и отказоустойчивости. Как говорилось в самом начале, данный документ призван создать основу для многостороннего обсуждения предлагаемых инициатив, обязанностей ICANN по созданию предлагаемых возможностей и способов организации усилий сообщества по оказанию поддержки таких инициатив. Выявлена потребность в значительных кадровых и материальных ресурсах, но возможные альтернативы финансирования данных инициатив не анализируются. В данном документе не предполагается, что ICANN будет финансировать эти инициативы или предоставлять для них сотрудников.

5.2 Инициатива 2 о необходимости установить DNS-CERT представлена более подробно в экономическом анализе DNS-CERT, сопровождающем данный документ.

5.1 Инициатива 1 - общесистемный анализ рисков DNS, планирование и учения на случай чрезвычайных обстоятельств

5.1.1 ICANN будет сотрудничать с сообществом DNS для профилактического понимания ключевых рисков для DNS, включая анализ возникающих угроз и рисков, как предусмотрено в подтверждении обязательств. После анализа этих рисков DNS сообщество должно определить чрезвычайные ситуации, представляющие наибольший интерес для общесистемной безопасности, стабильности и устойчивости DNS, и обеспечить наличие ресурсов для планирования в целях смягчению последствий выявленных рисков. ICANN считает, что в рамках своих обязанностей согласно утверждению обязательств она играет важную роль в обеспечении общесистемного планирования и учений на случай чрезвычайных обстоятельств. Такая активная программа должна дополнять мощности реагирования, которые могут быть предоставлены DNS-CERT в дополнение к использованию организации в качестве естественного центра для поддержки планирования на случай чрезвычайных ситуаций и учений.

5.1.2 Первым аспектом данной инициативы является подготовить основанный на сообществе подход к анализу риска, включающий принятую структуру риска DNS и оттачивающий подход к оценке рисков. Данные усилия подразумевают создание подхода к проведению регулярной оценки рисков DNS и к предложениям по смягчению последствий. Они опираются на работу симпозиума по безопасности, стабильности и отказоустойчивости DNS за 2010 год, а также на усилия DNS-OARC, ENISA и других.

5.1.3 Ещё одним аспектом данной инициативы является укрепление сотрудничества по всему сообществу в области планирования на случай чрезвычайных ситуаций и его использования в качестве основы для направления усилий по подготовке мощностей реагирования. Основа для планирования на случай чрезвычайных

обстоятельств должна начинаться с консенсуса по структуре общесистемных рисков DNS, определяющей главные риски для DNS и основные сценарии. Эта работа будет опираться на существующие усилия, как те, что реализуются в рамках государственно-частных партнёрств, занимающихся защитой важнейших объектов инфраструктуры, таких как координационный совет сектора информационных технологий США и ENISA, а также в рамках оперативного сообщества DNS, как DNS-OARC и NL Net Labs. Предлагаемая инициатива также предусматривает тесное сотрудничество с новым механизмом обмена информацией системы корневых серверов и с операторами реестров ДВУ. Анализ рисков и основных чрезвычайных обстоятельств будет использован для оценки адекватности существующих механизмов реагирования, определения недостатков, требующих исправления, а также подготовки планов для выявленных случаев. Усилия должны поддерживаться постоянной, объединяющей всё сообщество консультативной экспертной / рабочей группой. ICANN берёт на себя ответственность за поддержку группы и разработку плана действий для анализа сообщества, который станет вкладом в годовой цикл составления бюджета ICANN по безопасности, стабильности и отказоустойчивости и оперативному планированию.

5.1.4 После создания механизма планирования на случай чрезвычайных обстоятельств требуется общесистемная программа учебных проверок DNS для обеспечения оценки средств реагирования и определения их недостатков.[5] Как и в случае с DNS-CERT и усилиями по планированию на случай чрезвычайных обстоятельств, разработка программы учебных проверок должна опираться на существующую деятельность и включать такие инициативы, как существующие усилия по проведению учебных проверок ДВУ на случай чрезвычайных обстоятельств, в качестве суб-элементов более широкой программы. Необходимо поставить цель начать программу деятельности, кульминирующую проводимой два раза в год общесистемной учебной проверкой DNS, сосредоточенной на реакциях на основные чрезвычайные обстоятельства. Кроме того, программа должна включать интеграцию с другими программами, такими как серия многонациональных учебных проверок "cyber storm" (кибершторм) и прочими многосторонними международными учебными проверками. Как указывается в подтверждении обязательств, ICANN несёт ответственность за поддержку охватывающего всё сообщество подхода к этой программе, путём поддержки необходимых элементов программы и организации общесистемных учебных проверок DNS два раза в год.

5.1.1 Конкретные предлагаемые меры

5.1.1.1 Создание экспертно-консультативной группы по оценке рисков для DNS и планированию на случай чрезвычайных обстоятельств. Эта группа должна состоять из экспертов, представляющих сообщества деятельности DNS и кибербезопасности. ICANN должна осуществлять поддержку группы сотрудниками. Основное внимание группы должно быть сосредоточено на создании приемлемых для всего сообщества рамок системных рисков DNS и определении существующих

[5] Требования к такой программе для DNS определены отдельно в оценке рисков сектора ИТ DHS.

ключевых рисков к 3- кварталу 2010 г. Кроме того, группа должна опираться на работу симпозиума DNS SSR за 2010 год по показателям для создания приемлемых для всего сообщества рамок для определения состояния, безопасности, стабильности и отказоустойчивости DNS к началу 2011 г. Эта группа также должна отвечать за создание базовых плановых сценариев на случай чрезвычайных обстоятельств ко 2 кварталу 2011 г. Группа должна будет подготавливать ежегодный отчёт о рисках для DNS и их уменьшении, а первый отчёт должен будет быть представлен в 3 квартале 2011 г.

5.1.1.2 Создание механизма обмена информацией системы корневых серверов DNS должно стать плодом совместных усилий с сообществом операторов корневых серверов и прочими участниками сообщества корневых серверов на основе рекомендаций исследования по масштабированию корневой зоны за 2009 г. Будет сформирована рабочая группа, поддерживаемая сотрудниками ICANN, для определения функциональных требований и требований к мониторингу деятельности. К основным способностям должны относиться совершенствование моделирования системы корневых серверов DNS, улучшение обмена информацией между организациями, участвующими в системе корневых серверов, потенциальное развертывание необходимых датчиков, выделенная аналитическая поддержка оценки текущего состояния системы корневых серверов DNS и обеспечение предупреждений о возникающих проблемах. Будут предприниматься усилия по работе с сообществом с целью внедрения и развертывания датчиков и измерения показателей, которые позволят осуществлять обзор корневых серверов, системы ДВУ и её поведения. Эта работа потребует сотрудничества с операторами ДВУ, операторами корневых серверов, Национальным управлением по телекоммуникациям (NTIA), ICANN и прочими участниками операции и управления ключевой инфраструктурой DNS. Мы предполагаем, что данная система будет создана на основе взаимной поддержки параллельно с развитием DNS-CERT.

5.1.1.3 Продолжение поддержки планирования и учебных проверок на случай чрезвычайных обстоятельств операторов корневых серверов. После успешных учебных проверок связи и первоначальных настольных испытаний ко второй половине 2010 года ICANN запланирует работу с операторами по внедрению программного подхода к планированию на случай чрезвычайных обстоятельств и учебных проверок на основе сценариев. ICANN будет развёртывать коммуникационные мощности, которые будут дополнять и укреплять существующие системы, используемые в её деятельности, связанной с корневыми серверами.

5.1.1.4 Продолжение развития планирования и учебных проверок преемственности ДВУ. ICANN и операторы реестров ДВУ должны провести тестирование передачи данных на ответственное хранение в 2010 и 2011 годах на основе разработки спецификаций передачи данных на ответственное хранение для механизма новых родовых доменов верхнего уровня (рДВУ). Дополнительно планируются учения с упором на элементы связи и реагирования на кризис между ICANN и операторами реестров ДВУ.

5.1.1.5 Инициировать развитие общей для DNS программы учебных проверок и оценки. Такая программа должна включать использование существующих усилий и потребует участия широкого круга субъектов, включая тех, кто участвует в операциях DNS, сообществ поставщиков и пользователей DNS и более широкое сообщество кибербезопасности. Эта программа будет также включать исследование и использование точек пересечения с другими программами кибербезопасности и связанными с ними программами учебных проверок и оценки. К концу 2010 года эти усилия позволят оценить характер и адекватность принимаемых мер и определить основные пробелы. К середине 2011 года на общественное обсуждение будет вынесена концепция программы упражнений для DNS. Кроме того, ICANN будет спонсировать ограниченную общесистемную учебную проверку во второй половине 2011 года в качестве прототипа с добровольным участием всех субъектов, заинтересованных в формировании долгосрочных процессов планирования и исполнения. Планирование этой прототипной учебной проверки начнётся в 2010 году. Сотрудники ICANN и прочие участники сообщества DNS примут участие в многосторонних учениях Cyber Storm III, а также могут участвовать в других международных учениях.

5.1.2 Предполагаемые ресурсы

5.1.2.1 Проецируется необходимость пяти должностей сотрудников на полной ставке:

- Старший координатор, оценка рисков, планирование на случай чрезвычайных обстоятельств и программа учений;
- Координатор планирования на случай чрезвычайных обстоятельств;
- Координатор программы учений и оценки;
- Составитель плана учений;
- Системный аналитик / эксперт по моделированию корневой системы, система обмена информацией корневой системы.

5.1.2.2 Требования по поддержке включают определение требований по обмену информацией с системой корневых серверов; поддержку анализа риска и усилий по обмену информацией с корневыми серверами; инфраструктуру и связанные с ней расходы, к которым относятся лицензирование и программно-аппаратная поддержка моделирования, система обмена информацией и связи с корневыми серверами и прототипное развёртывание системы датчиков; командировочные расходы и расходы на совещания рабочих групп и персонала; объекты инфраструктуры и ИТ-поддержку для дополнительных сотрудников.

5.1.2.3 Мы ожидаем, что расходы на поддержку этих усилий с июля 2010 по июнь 2011 года составят около 1,25 млн. долл. США на сотрудников и 850 тыс. долл. США на поддержку. Общие прогнозируемые расходы на реализацию этой инициативы за первый год составят 2,1 млн. долл. США.

5.1.2.4 **Предположения:** При анализе рисков будет использоваться информация об угрозах и их анализ из DNS-CERT. Система обмена информацией с корневыми

серверами позволит использовать портал Web 2.0, разработанный для DNS-CERT для поддержки обмена информацией.

5.2 Инициатива 2 - DNS-CERT

5.2.1 Помимо активной оценки рисков, планирования и проведения учебных проверок сообществу DNS требуются эффективные, оперативные, общесистемные средства адекватного реагирования на проблемы, связанные с безопасностью, стабильностью и отказоустойчивостью. Широкомасштабное координированное нападение на DNS может привести к значительным экономическим и политическими последствиями, но при этом для DNS не существует центрального пункта связи на случай чрезвычайных обстоятельств для координации технических действий и политики, связанной с определением и координацией реагирования на такие инциденты. В 2009 году на всемирном симпозиуме по безопасности, стабильности и отказоустойчивости DNS были особо отмечены задержки реагирования на нарушения безопасности в DNS и рекомендованы меры по их устранению. Кроме того, многие операторы DNS не обладают достаточными ресурсами и, как следствие, имеют ограничения при разработке надежных средств безопасности и отказоустойчивости. Эти организации могут не знать, куда обратиться за помощью, или же страдать от языковых или географических барьеров, препятствующих получению помощи. Высока вероятность уязвимости таких организаций и их использования для нанесения вреда DNS в целом. ICANN считает, что необходим центральный узел связи, DNS-CERT, для обеспечения технической координации и координации политики для DNS и для работы с сообществом DNS по определению и координации реагирования на глобальные происшествия в DNS.

5.2.2 DNS-CERT будет координировать предпринимаемые усилия с сообществом DNS для поддержания ситуационной осведомлённости, с тем, чтобы любой член всего сообщества мог легко и в любое время найти требуемый источник информации. Основными субъектами данных усилий являются операторы и пользователи DNS, поставщики, исследователи в области безопасности, а также специалисты по реагированию на чрезвычайные обстоятельства. DNS-CERT позволит привлечь ряд существующих усилий, направленных на выявление угроз, обмен информацией и содействие реагированию через DNS. Деятельность DNS-CERT может помочь в плане сотрудничества и содействия координации этих усилий, предоставлении услуг в областях, которые в настоящее время не охвачены, или субъектам, не участвующим в данных мероприятиях. DNS-CERT может быть запущен с поддержкой ICANN, но конкретная организационная структура и модель обеспечения ресурсами будет определяться на основе диалога с обществом. В связи с этим, контроль за DNS-CERT будет осуществлять Совет из спонсоров, что обеспечит подотчётность постоянной группе CERT, а также позволит оценивать деятельность DNS-CERT с учётом потребностей заинтересованных сторон, которым данная организация предоставляет услуги. Деятельность DNS-CERT будет осуществлять ключевая группа административно-технических сотрудников, которым будет содействовать расширенный коллектив, состоящий из виртуальных

специалистов, которые будут оказывать существенную поддержку DNS-CERT, работая в географически распределённом режиме.

5.2.3 DNS-CERT будет обеспечивать как активные (то есть, анализ угроз, мониторинг состояния и безопасности DNS, ситуационную осведомлённость и обмен информацией), так и реактивные услуги (т.е. точка круглосуточного и ежедневного контакта, координация управления инцидентами, поддержка управления уязвимостями и консультативные услуги в области безопасности) для своих постоянных субъектов. Такой подход важен по двум причинам: (1) активная информация о картине существующих угроз может помочь сообществу DNS принимать их во внимание посредством профессиональной подготовки и учебных проверок; а (2) услуги реактивного управления инцидентами могут помочь субъектам, испытывающим значительную нехватку ресурсов, таким как регистраторы в менее развитых регионах земного шара. Информация об угрозах и их анализ будут также способствовать прогнозируемому создания средств выявления и анализа системных рисков в DNS, описанных в рамках инициативы 1. Функциональные требования к основным возможностям, которые будет предоставлять DNS-CERT, будут определяться сообществом в ходе анализа с участием заинтересованных субъектов и возможных сотрудников DNS-CERT.

5.2.2 Предполагаемые ресурсы

5.2.2.1 На основе оценки национальных коллективов CERT аналогичного размера и уровня ответственности мы считаем, что DNS-CERT может начать функционировать с годовым бюджетом, обеспечивающим около 15 сотрудников, с учётом директора, двух старших руководителей, группы управления инцидентами из десяти человек, а также сотрудников администрации и юридической поддержки. Прогнозируемые расходы на персонал составляют 2,6 млн. долл. США. Расходы на командировки персонала, средства связи и инструменты анализа, материальное обеспечение и ИТ-поддержку оцениваются в 1,6 млн. долл. США. Общая расчетная сумма расходов за первый год реализации данной инициативы составляет 4,2 млн. долл. США. Подробная информация представлена в экономическом анализе DNS-CERT, прилагаемом к данному документу.

6. Заключение

Задачи по обеспечению безопасности, стабильности и отказоустойчивости DNS всё растут. В соответствии со своим уставом и подтверждением обязательств ICANN несёт значительные обязательства по обеспечению работы с сообществом DNS по решению этих проблем. В частности, требуется создание общесистемных средств планирования на случай чрезвычайных обстоятельств, учебных проверок и совместного реагирования для DNS. Этот концептуальный документ предоставляет основу для многостороннего обсуждения предлагаемых инициатив по обеспечению выполнения данных требований.