The Internet Corporation for Assigned Names and Numbers

Сводная информация о последствиях масштабирования корневой зоны

Дата публикации: октябрь 2010 г.

Сводная пояснительная записка

В феврале 2009 г. Правление ICANN направило запрос на проведение исследования с целью изучить последствия использования ряда новых технологий и потенциальной возможности добавления существенного количества новых доменов верхнего уровня в корневую зону DNS. Хотя некоторые из этих технологий к тому времени уже были частично развернуты, сообщество выразило определенную озабоченность в связи с риском нарушения стабильности DNS в случае внедрения этих изменений и дополнений без соблюдения осторожности. По запросу Правления ICANN были проведены два исследования, в центре одного из которых находилось влияние новых технологий и добавления ДВУ на один из серверов корневой зоны, а в ходе другого широко рассматривались все процессы, связанные с управлением корневой системой.

Вызывающие интерес новые технологии включали протокол IPv6 (как в отношении адресов IPv6, связанных с доменами верхнего уровня и корневыми серверами, так и в отношении поддержки запросов IPv6, отправленных на корневые серверы), интернационализированные доменные имена (ИДИ) и усовершенствования системы безопасности DNS (DNSSEC). Однако поскольку после принятия резолюции Правления ICANN (а в некоторых случаях и раньше) все эти технологии были развернуты или внедрены в корневой зоне, существуют некоторые эмпирические данные, которые можно использовать для понимания влияния этих технологий.

К настоящему времени развертывание IPv6, DNSSEC и ИДИ в корневой системе не оказало существенного вредного влияния. Хотя развертывание этих новых технологий, возможно, привело к некоторому незначительному ухудшению услуг из-за отсутствия устойчивой инфраструктуры IPv6 и/или большего размера ответов (по причине добавления записей IPv6 или подписей DNSSSEC в корневой зоне), являющегося причиной потери ответов и, как следствие, превышения времени ожидания и необходимости повторных передач, не наблюдалось существенных последствий, которые могли бы вызвать озабоченность соответствующих сообществ.

В перспективе, исходя из предположения, что верхний предел ежегодного добавления менее 1000 новых рДВУ в корневую зону определен точно, а также предположив, что остальные параметры, относящиеся к управлению корневой зоной DNS, не претерпят существенных изменений, представляется вероятным, что стандартные циклы функционального

обновления и распределения ресурсов будут достаточными для обеспечения того, что масштабирование корневой зоны как в отношении новых технологий, так и в отношении нового содержимого не окажет существенного влияния на стабильность корневой системы.

Однако понимая, что в управлении корневой зоной DNS принимает участие множество сторон, а также в интересах максимально осторожного подхода к обеспечению стабильности корневой зоны DNS необходимо улучшить мониторинг системы управления корневой зоной, особенно в областях, наиболее чувствительных к изменениям темпов роста или требующих существенного времени на подготовку к таким изменениям. Кроме того, более четкое и частое взаимодействие между соответствующими партнерами по управлению корневой зоной и другими заинтересованными сторонами, включая официальное информационное взаимодействие между персоналом ICANN и операторами корневых серверов по вопросам планируемого количества одобренных заявок, дополнительных технологий, которые необходимо развернуть, сроков развертывания и т. п., вероятно, повысит уверенность в том, что изменения в корневой системе не окажут отрицательного влияния на стабильность этой системы.

Введение

В период 2004–2010 гг. корневая зона DNS подвергается существенному изменению, как в отношении содержимого, так и в отношении вспомогательной инфраструктуры. Можно с уверенностью сказать, что за последние 5–6 лет с добавления в корневую зону интернационализированных доменных имен (ИДИ) и до развертывания IPv6 и DNSSEC произошло больше изменений, чем со времени первого развертывания DNS. С неизбежным принятием заявок на новые родовые домены верхнего уровня (рДВУ) можно ожидать дальнейших существенных изменений в корневой зоне DNS.

В соответствии с миссией ICANN «обеспечивать стабильное и надежное функционирование систем уникальных идентификаторов Интернета»[1] Правление ICANN направило запрос на выполнение Консультативным комитетом системы корневых серверов ICANN (ККСКС) и Консультативным комитетом ICANN по безопасности и стабильности (ККБС) при поддержке руководящих сотрудников ICANN совместного исследования для изучения влияния предлагаемых изменений корневой системы DNS. Однако как до,

[1] Источник: «Статья 1, Раздел 1. Миссия» Устава ICANN, см. http://www.icann.org/en/general/bylaws.htm

так и во время проведения этого исследования многие представляющие интерес для Правления изменения корневой системы были уже внедрены без заметных отрицательных последствий.

В настоящем документе представлена сводная информация об изменениях, произошедших в корневой зоне DNS, и анализ этих изменений наряду с оценками предполагаемого влияния будущих изменений, в том числе добавления новых доменов верхнего уровня.

Историческая справка

3 февраля 2009 г. Правление ICANN в резолюции 2009-02-03-04[2] приняло единогласное решение о проведении совместного исследования ККСКС и ККБС с целью анализа «*влияния предложений по внедрению [IPv6, ДВУ с ИДИ, DNSSEC и новых рДВУ] на безопасность и стабильность системы корневых серверов DNS».* В этой резолюции сформулированы следующие задачи совместного исследования:

- «*[Р]ассмотреть последствия первичного внедрения этих изменений, наблюдаемые в течение сокращенного периода времени.»*
- «*[Р]ассмотреть возможности и масштабирование системы корневых серверов с целью решения широкого диапазона технических проблем и удовлетворения функциональных потребностей, которые могут возникнуть в рамках внедрения предлагаемых изменений.»*
- «*[С]формулировать техническое задание на проведение исследования и назначить руководящий комитет для координации этих усилий к 28 февраля 2009 г.»*
- «*[О]беспечить непосредственное участие соответствующего руководящего технического персонала ICANN в запланированных к проведению мероприятиях и обеспечить необходимую поддержку различных аспектов проведения этого исследования в надлежащие сроки и при окончательном утверждении консультативными комитетами.»*
- Обеспечить, чтобы *«процесс определения сроков, характера и реализации исследования учитывал изложенные технические и функциональные проблемы в отношении расширения корневой зоны DNS».*
- Представить Правлению ICANN *«выводы и рекомендации по результатам исследования к 15 мая 2009 года».*

В результате этого решения были предприняты усилия в двух направлениях: исследование, сосредоточенное на влиянии масштабирования корневой зоны на один из корневых серверов (корневой сервер «L», находящийся под управлением ICANN), и более общее исследование, нацеленное на моделирование процессов в

[2] См. http://www.icann.org/en/minutes/prelim-report-03feb09.htm

системе управления корневой зоной и анализ результатов масштабирования этой системы. Для выполнения второго исследования была сформирована специальная исследовательская группа, известная как «Комитет по вопросам масштабирования корневых серверов» (КМКС), в состав которой вошли члены ККСКС и ККБС, а также сторонние эксперты.

Исследование корневого сервера «L»

Исследование корневого сервера «L», выполненное операционным и исследовательским центром системы доменных имен (DNS-ОАИЦ) по договору с ICANN, было сосредоточено на оценке последствий добавления IPv6, DNSSEC и новых ДВУ в различных сочетаниях в рамках лабораторного моделирования поведения корневого сервера «L». Итоговый отчет по результатам данного исследования, озаглавленный «Расширение корневой зоны и анализ последствий», был опубликован 17 сентября 2009 г. и доступен по адресу http://www.icann.org/en/topics/ssr/root-zone-augementation-analysis-17sep09-en.pdf.

Исследование КМКС

В ходе исследования КМКС, где результаты исследования корневого сервера «L» использовались как часть исходных данных, были привлечены внешние ресурсы для моделирования процессов управления корневой зоной и проведения интервью с операторами корневых серверов, персоналом IANA, VeriSign, NTIA и других организаций. Это исследование имело намного более общий характер и было нацелено на анализ влияния не только на корневые серверы, но также и на системы обеспечения, подготавливающие распространение корневой зоны на корневые серверы. Итоговый отчет по результатам данного исследования, озаглавленный «Масштабирование корневой зоны» с подзаголовком «Отчет о влиянии увеличения размеров и изменчивости корневой зоны на корневую систему DNS», был опубликован 31 августа 2009 г. и доступен по адресу http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf.

События в области масштабирования корневой зоны

До и после того как Правление ICANN направило запрос ККБС, ККСКС и руководящим сотрудникам ICANN на исследование последствий масштабирования корневой зоны, многие предметы этого исследования уже были внедрены. Сроки внедрения новых технологий в корневой зоне представлены в *Таблица 1*.

Дата	Технология	Событие
июль 2004 г.	IPv6	Первые адреса IPv6 добавлены в корневую зону для доменов верхнего уровня (KR и JP).
ноябрь 2005 г.	DNSSEC	Подписан первый домен верхнего уровня (.SE).
июнь 2007 г.	DNSSEC	Стала доступной испытательная модель IANA для подписей DNSSEC в корневой зоне.
август 2007 г.	ИДИ	В корневую зону добавлены пробные домены верхнего уровня с ИДИ.
февраль 2008 г.	IPv6, рДВУ	Добавлены первые адреса IPv6 для корневых серверов (A, F, J, K, L и M). Исходя из оценки времени обработки рДВУ, определен предел, не превышающий 1000 новых рДВУ в год.
январь 2010 г.	DNSSEC	На первом корневом сервере («L») опубликована зона, которая заведомо не может быть криптографически проверена (DURZ).
май 2010 г.	ИДИ, DNSSEC	В корневую зону добавлены первые эксплуатируемые в производственном режиме ИДИ (для Египта, Саудовской Аравии и Объединенных Арабских Эмиратов). Зона DURZ развернута на всех 13 корневых серверах.
июнь 2010 г.	DNSSEC	В корневой зоне опубликованы первые записи DS (для .UK и .BR).
июль 2010 г.	DNSSEC	Корневая зона получила подпись DNSSEC, и опубликована отметка о доверии для корневой зоны.

Таблица 1 — события в области масштабирования корневой зоны

Последствия

В период с июля 2004 г., когда в корневую зону были добавлены первые адреса IPv6 для серверов имен ДВУ, и до DNSSEC-подписания корневой зоны и введения в корневую зону записей DS в июле 2010 г. обслуживание в корневой зоне DNS продолжалось без каких-либо сообщений об ухудшении или заметных ухудшений качества обслуживания в связи с указанными событиями. В настоящем разделе рассматривается влияние различных изменений по отдельности на корневую зону DNS.

IPv6

Включение IPv6 в корневую зону DNS состоит из двух компонентов: добавление в корневую зону «связующих» записей[3] IPv6 для полномочных серверов имен ДВУ и добавление «связующих» записей IPv6 к корневым серверам. Последствия каждого из указанных событий будут рассмотрены по очереди.

Домены верхнего уровня

Первыми ДВУ, к которым в июле 2004 г. были добавлены «связующие» записи IPv6, стали домены .JP и .KR. По состоянию на 6 сентября 2010 г. в корневой зоне имеется 283 «связующих» записи IPv6, охватывающие 203 ДВУ. Одним из последствий более широкого использования «связующих» записей IPv6 стал рост количества разрешений с использованием транспорта IPv6. По состоянию на 6 сентября 2010 г. по крайней мере на один из корневых серверов (корневой сервер «L») поступает приблизительно 1,3% запросов DNS по протоколу IPv6[4]. Поскольку в настоящее время сетевая инфраструктура IPv6 имеет в Интернете меньшую устойчивость, запросы и/или ответы IPv6 могут теряться чаще, чем для протокола IPv4, что приводит к увеличению количества случаев превышения времени ожидания и повторных передач, по сравнению с тем временем, когда в ДВУ не поддерживался протокол IPv6. Однако это влияние имеет минимальные отрицательные последствия, и ожидается улучшение ситуации по мере более широкого развертывания IPv6.

Корневые серверы

Когда некоторые операторы корневых серверов добавили адреса IPv6 для своих записей корневых серверов имен, размер «инициирующего запроса» существенно увеличился. Как обсуждалось в отчете SAC018, составленном совместно ККСКС и ККБС и озаглавленном «Аккомодация записей ресурсов адресов IP версии 6 для корня доменной системы имен»[5], возникла озабоченность в связи с ожиданием того, что размер ответа на инициирующий запрос превысит размер «классического» не усеченного максимального ответа DNS в 512 байт. Существовали опасения, что, если распознаватель, запрашивающий инициирующий ответ, не обеспечит больший размер буфера для ответа через расширение EDNS0[6], корневые серверы могут указать усеченный ответ, что

---

[3] Связующими записями являются записи ресурсов IPv4 («A») и IPv6 («AAAA»), связанные с серверами имен, находящимися в просматриваемой зоне. Определение связующих записей см. в RFC 1034 (http://www.ietf.org/rfc/rfc1034.txt).

[4] Личные беседы с операторами корневого сервера «L». Процент запросов для других корневых серверов должен быть аналогичным.

[5] См. http://www.icann.org/en/committees/security/sac018.pdf

[6] Расширение EDNS0 определено в RFC 2671 (см. http://www.ietf.org/rfc/rfc2671.txt).

приведет к повторной передаче распознавателем запроса по TCP. Поскольку запросы DNS на основе TCP используют ресурсы значительно интенсивнее стандартных запросов на основе UDP, существовала определенная озабоченность возможностью перегрузки корневых серверов, приводящей к снижению качества обслуживания всех пользователей, направляющих запросы на корневые серверы. Кроме того, существовала некоторая озабоченность, что больший по размеру ответ корневых серверов будет блокироваться или отфильтровываться брандмауэрами, устройствами трансляции сетевых адресов (NAT) и прочими «промежуточными» устройствами, которые (ошибочно) «знают», что размер ответа DNS никогда не может превышать 512 байт. В таких случаях возникал риск неполучения ответа на запрос и, следовательно, невозможности получения адресов корневых серверов.

После объемных исследований и диагностики этой проблемы в феврале 2008 г. адреса IPv6 были добавлены в корневую зону. На практике реализации серверов DNS, работающих в корневой зоне, исключали несущественную информацию («дополнительный раздел») вместо усечения ответов на запросы, в которых не был указан значительно больший размер буфера через EDNS0 (или не использовалось расширение EDNS0). Возможно, это привело к небольшому росту количества запросов к корневым серверам, поскольку распознаватели должны были направлять дополнительные запросы для получения данных, которые ранее были представлены в дополнительном разделе. Однако, если это и произошло, рост количества запросов не был заметным.

Для тех запрашивающих устройств, которые предоставляли значительно больший размер буфера через расширение EDNS0, возможно, выросло количество фрагментированных пакетов, что могло привести к потере ответов либо из-за потери фрагмента, либо из-за настройки промежуточных устройств на отклонение фрагментов. Кроме того, некоторые политики безопасности (ошибочно) подразумевают, что запросы DNS на основе TCP должны быть заблокированы. В этих случаях инициирующий запрос без параметра EDNS0 (или запрос, в котором предложенный размер буфера меньше размера ответа) может привести к блокировке ответа. Однако за более чем два с половиной года со времени установки в корневой зоне первых «связующих» записей IPv6 для корневых серверов не появлялись существенные (или вообще какие-либо) отчеты об отрицательных последствиях.

Если рассмотреть обрабатывающую часть системы управления корневой зоной, потребовалась некоторая модификация процессов и систем ICANN для управления корневой зоной, а также процессов и систем VeriSign, с целью обработки записей ресурсов IPv6 «AAAA» и проверки доступности IPv6 в ходе «технических проверок», выполняемых обеими сторонами. Однако последствия как для ICANN, так и для VeriSign оказались минимальными, и эти процессы и системы продолжают функционировать сегодня без происшествий.

Интернационализированные доменные имена (ИДИ).

Что касается DNS, то помимо незначительно увеличившейся средней длины метки, интернационализированные доменные имена по сути неотличимы от любых других доменных имен. Таким образом, для DNS добавление ИДИ в корневую зону ничем не отличалось от добавления в корневую зону любых других ДВУ, не являющихся ИДИ. В силу этого на уровне DNS не наблюдалось никакого влияния.

Однако было оказано некоторое влияние на процессы и системы ICANN для управления корневой зоной. Для отображения информации ИДИ в пригодном для использования виде персоналу IANA потребовалось пересмотреть процессы для запроса U-меток помимо A-меток, а также модифицировать системы IANA, например сервер WHOIS, для поддержки отображения и A-меток, и U-меток. В общем, поддержка ИДИ во вспомогательных системах, особенно при отображении данных владельцев регистрации, остается актуальной темой, которая обсуждается в настоящее время (наряду с другими, например, имеющими отношение к безопасности) на форумах ICANN. Можно ожидать, что необходимость правильного отображения информации ИДИ окажет в будущем существенное влияние (по крайней мере) на регистраторов.

DNSSEC

Добавление DNSSEC в корневую зону оказало серьезное влияние на размер корневой зоны и размер ответов на запросы к корневой зоне. Развертывание DNSSEC также имело определенные последствия для ICANN, VeriSign и NTIA — организаций, участвующих в управлении корневой зоной. В отношении размера корневой зоны по состоянию на 6 сентября 2010 г. можно сказать, что он составлял 222 246 байт (при проводной передаче всей зоны полностью). При удалении из зоны всех записей, имеющих отношение к DNSSEC, а именно записей ресурсов DNSKEY, NSEC, DS и RRSIG, размер зоны составлял 122 657 байт. Однако на основе данных, полученных в ходе исследования корневого сервера «L», ожидалось, что для любого правильно настроенного сервера имен дополнительная нагрузка со стороны DNSSEC при передаче данных будет несущественной, и это подтвердилось на практике: не поступало отчетов о каких-либо трудностях, возникших у операторов корневых серверов в связи с загрузкой и обслуживанием зоны с подписью DNSSEC во время развертывания «зоны, которая заведомо не может быть криптографически проверена (DURZ)» в рамках поэтапного развертывания DNSSEC в корневой зоне перед опубликованием отметки о доверии для корневой зоны.

Потенциально, более важное значение имеет существенный рост размера большинства ответов от корневых серверов. Например, при запросе ответа с подписью DNSSEC он вырос для корневых серверов имен с 492 байт до 829 байт. В противоположность размеру данных зоны, удвоение размера ответа DNS вызвало

озабоченность из-за ограничения в 512 байт, которое было рассмотрено ранее в контексте IPv6. В спецификациях DNSSEC это ограничение было учтено введением требования использовать EDNS0 для сигнализации о том, что распознаватель имеет необходимое оснащение для обработки ответов, включающих записи ресурсов, связанные с DNSSEC. Однако, как оказалось, большинство распознавателей Интернета, по крайней мере, направляющих запросы к корневым серверам, используют EDNS0 по умолчанию и устанавливают бит в запросах DNS (бит «DNSSEC OK») в качестве указания на то, что этот распознаватель понимает ответы, включающие записи ресурсов, связанные с DNSSEC (независимо от того, использует ли данный распознаватель указанные записи ресурсов). В результате от 50% до 80% запросов, поступавших на корневые серверы до подписания корневой зоны, имели установленный бит «DNSSEC OK» и, следовательно, когда подписанная корневая зона стала обслуживаться всеми корневыми серверами, указанные серверы немедленно начали возвращать в совокупности не менее 50 000 записей ресурсов, связанных с DNSSEC, в секунду[7].

До подписания корневой зоны имелась существенная озабоченность в отношении последствий возврата ответов с подписью DNSSEC, имеющих больший размер, клиентам, которые их не ожидают. В частности, существовали опасения, что промежуточные устройства (аналогично рассмотренной выше ситуации с IPv6) будут отклонять ответы, размер которых превышает 512 байт. В результате, ICANN, VeriSign и NTIA пришли к соглашению о поэтапном развертывании подписанной корневой зоны (DURZ), которое также включало существенные объемы измерения параметров корневых серверов с целью отслеживания всех изменений в шаблонах запросов. Однако после развертывания подписанной корневой зоны на всех 13 корневых серверах в течение 6 месяцев ни одна из сторон, принимавших участие в подписании корневой зоны, не получила ни одного отчета об отрицательных последствиях.

Что касается изменения процессов, развертывание DNSSEC в корневой зоне привело к созданию новых продуманных процессов и физических объектов, необходимых для безопасного управления ключом ICANN для подписания ключей и ключом VeriSign для подписания корневой зоны. Также были созданы новые процессы, позволяющие администраторам ДВУ безопасным образом предоставлять в ICANN сведения о «подписывающем устройстве делегирования» (DS) и позволяющие ICANN направлять сведения о DS компании VeriSign для включения в корневую зону, чтобы обеспечить возможность создания «цепочки доверия» от корневой зоны к подписанным дочерним зонам. До настоящего времени эти новые процессы работали без происшествий.

[7] Исходя из приблизительной средней оценки в размере 8000 запросов в секунду на один кластер корневых серверов в 13 кластерах корневых серверов и при условии, что бит «DNSSEC OK» установлен в половине запросов.

Резюме

Суммируя последствия добавления IPv6 в корневую систему, ввода доменов верхнего уровня с ИДИ и развертывания DNSSEC, можно утверждать, что к настоящему времени не наблюдается никакого существенного вредного влияния этих событий, и отчеты о таком влиянии не поступали в ICANN.

Однако, вместе с тем, одним из вопросов, поднятых в контексте обсуждения масштабирования корневой зоны, является необходимость улучшения информационного взаимодействия между заинтересованными сторонами, принимающими участие в управлении корневой системой. В некоторых случаях процесс внедрения новых технологий, вероятно, можно улучшить за счет более формального обмена информацией о требованиях всех сторон, на которые может быть оказано влияние, обсуждения этих требований и последствий, документального оформления планов с указанием сроков и т. п. Обмен информацией, подготовку документов и обсуждение в рамках развертывания подписанной корневой зоны предложено использовать в качестве примера движения в правильном направлении.

Прогнозы

Изменения в корневой зоне продолжатся, хотя теперь в большей степени в рамках дальнейшего развертывания существующих технологий, чем в рамках структурных изменений, таких как внедрение новых технологий. В настоящем разделе рассматриваются некоторые прогнозы в отношении вероятных изменений, в предположении, что такие параметры как время обновления зоны, значения времени актуальности записи DNS (TTL), темп изменений в корневой зоне, а также продолжительность и сложность административных процедур не претерпят значительных или неожиданных изменений по сравнению со своими историческим значениями.

IPv6

В будущем, с высокой степенью вероятности, новые домены верхнего уровня добавят записи адресов IPv6 для своих серверов имен. По состоянию на 6 сентября 2010 г. корневая зона содержит 283 «связующих» записи IPv6, которые соответствуют 203 из 294 доменов верхнего уровня, имеющим по крайней мере одну запись адреса IPv6 для своих серверов имен. Можно с уверенностью предположить, что по мере более полного развертывания IPv6 большее количество ДВУ добавит поддержку IPv6, что в конечном итоге приведет к охвату всех ДВУ, а среднее количество серверов имен, поддерживающих IPv6, для этих ДВУ будет расти. До тех пор, пока инфраструктура IPv6 Интернета не улучшится до уровня инфраструктуры IPv4, конечные пользователи могут испытывать некоторые отрицательные последствия в виде задержек по причине истечения времени ожидания ответов на запросы, отправленные серверам имен IPv6.

В случае корневой зоны в документе SAC018 указано, что размер ответа на инициирующий запрос после развертывания IPv6 на всех корневых серверах должен составлять 811 байт. Хотя операторы корневых серверов, еще не осуществившие развертывание IPv6, не предоставили сведения о датах, к которым они планируют включить поддержку IPv6 на своих корневых серверах, все они выразили намерение использовать этот протокол[8]. Однако поскольку уже встречаются ответы, размер которых превышает 512 байт, маловероятно, что дополнительные 100+ байт в ответе на инициирующий запрос окажут существенное влияние.

DNSSEC

По состоянию на 15 июля 2010 г. корневая зона была подписана и распространяется на все экземпляры всех 13 корневых серверов. По этой причине дальнейшее влияние на корневую зону со стороны DNSSEC, вероятно, будет ограничено добавлением, изменением и удалением записей ресурсов подписывающих устройств делегирования (DS), возможными изменениями алгоритмов, длины или количества ключей, а также мероприятиями по смене ключей.

Поскольку записи ресурсов DS могут иметь переменный размер в зависимости от используемого алгоритма хеширования, трудно с точностью предсказать степень увеличения размера записей DS в будущем. Однако, принимая во внимание структуру записей ресурсов DS, можно аргументированно доказать, что по пессимистичной оценке размер записи DS составит 64 байта. По состоянию на 6 сентября 2010 г. имеется 49 записей DS для 29 ДВУ (включая 11 пробных ДВУ с ИДИ, все еще находящихся в корневой зоне). Предположив, как и в исследовании корневого сервера «L», что полное развертывание записей DS доменами верхнего уровня приведет к общему количеству в 1440 записей ресурсов DS для 1000 зон, общий объем, добавленный записями DS, составит менее 100 килобайт. Вероятно, фактический объем будет существенно меньше, поскольку он привязан к количеству ДВУ, и (как обсуждается в следующем разделе) ожидается, что это количество будет намного меньше 1000 новых ДВУ — предположения, использовавшегося в исследовании корневого сервера «L».

В отношении изменения алгоритмов, длины и количества ключей возможно, что наиболее существенное изменение будет заключаться в переходе на криптосистему на основе эллиптических кривых, который приведет к использованию значительно меньших по размеру ключей с такой же криптографической стойкостью.

[8] Личные беседы с сопредседателем ККСКС и оператором корневого сервера «L».

И наконец, хотя это в большей степени является эксплуатационным вопросом, а не вопросом масштабирования корневой зоны, мероприятия по смене ключей будут проходить с определенной регулярностью во всех зонах, подписанных DNSSEC. При нормальном ходе событий смена ключей для подписания ключей потребует предоставления обновленных записей DS администратору родительской зоны. В случае корневой зоны смена ключа для подписания ключей в корневой зоне потребует обновления отметки о доверии для корневой зоны во всех определителях, настроенных на проверку подлинности. Выражается надежда, что механизмы на основе RFC 5011 позволят автоматизировать большинство операций смены ключа для подписания ключей, но можно ожидать некоторого нарушения работы при изменении ключа для подписания ключей и, следовательно, смену ключа для подписания ключей в корневой зоне следует выполнять с особой осторожностью.

Домены верхнего уровня

В ходе анализа, выполненного в проекте документа «Сценарии интенсивности делегирования новых рДВУ»[9], персонал ICANN оценил ожидаемую интенсивность делегирования новых ДВУ в корневой зоне на уровне от 200 до 300, даже при более высокой, чем ожидается, интенсивности подачи заявок. В том же документе сделано заключение, что независимо от количества заявок будет действовать присущее процессу ограничение на добавление новых ДВУ на уровне меньше максимального значения, равного 1000 новых рДВУ в год[10]. В целях данного анализа предполагается, что ежегодно будет добавляться фиксированное количество новых ДВУ, равное 1000.

На основе работы, выполненной в ходе исследования корневого сервера «L», ожидаемый размер корневой зоны с подписью DNSSEC, IPv6 и полным развертыванием DS при количестве новых доменов верхнего уровня 1000 составит 624 791 байт. С учетом комментариев, полученных от операторов корневых серверов, маловероятно, что такой объем данных зоны создаст серьезную нагрузку для какого-либо из корневых серверов. Кроме того, эта корневая зона должна быть распространена на каждый экземпляр всех 13 корневых серверов. В целях данного анализа, исходя из предположения, что эффективная минимальная пропускная способность (с учетом шума в линии передачи, прерывания связи и т. п.) для имеющего наихудшее подключение экземпляра всех корневых серверов составляет 300 бит в секунду, для передачи всей зоны потребуется четыре с

[9] См. http://www.icann.org/en/topics/new-gtlds/anticipated-delegation-rate-model-25feb10-en.pdf

[10] Более точно — 924 новых ДВУ в год.

половиной часа, что с большим запасом укладывается в 12-часовой период обновления корневой зоны[11].

В исследовании корневого сервера «L» содержится прогноз, что через 10 лет при сохранении предположения о максимальном количестве 1000 новых ДВУ в год корневая зона вырастет до 7 471 784 байт. Опять же, с учетом комментариев операторов корневых серверов, маловероятно, что такой объем данных зоны создаст серьезную нагрузку для какого-либо из корневых серверов. Что касается пропускной способности, минимальная пропускная способность, необходимая для передачи зоны такого размера в течение 12-часового окна составит приблизительно 1400 бит в секунду.

Другое возможное будущее последствие добавления новых ДВУ связано с «расширением» запросов к корневой зоне. То есть, рассеивание запросов между возросшим количеством ДВУ может оказать определенное влияние на работу отдельных серверов кэша. Хотя не очевидно, что рост количества ДВУ приведет к росту числа запросов или что шаблоны запросов радикально изменятся, если рассмотреть экстремальную ситуацию, когда распознаватель отправит запрос каждому ДВУ в корневой зоне, кэш такого распознавателя в итоге будет хранить записи NS для каждого ДВУ (наряду со «связующими» записями IPv4 и IPv6, а также записями, имеющими отношение к DNSSEC, если они существуют) в течение времени актуальности (TTL) таких записей. По сравнению с ограниченным количеством ДВУ в настоящее время, это приведет к увеличению объема памяти, используемого кэширующим сервером имен и, в зависимости от способов управления памятью кэширующего сервера имен, может повысить вероятность того, что кэширующий сервер имен израсходует всю доступную память. Однако кэширующие серверы имен уже сейчас сталкиваются с необходимостью решения проблем управления памятью такого вида, поскольку уже имеется достаточное количество доменных имен, к которым могут направляться запросы (на всех уровнях), в значительной степени переполняющие любую конфигурацию памяти, если эти запросы направляются достаточно быстро (то есть, в пределах времени TTL этих записей, так что количество добавляемых новых записей превышает количество записей с истекшим сроком действия). По этой причине не следует ожидать, что более высокая степень «расширения» в корневой зоне окажет в результате существенное влияние на кэширующие серверы.

Как обсуждалось в отчете КМКС, добавление новых доменов верхнего уровня, вероятно, окажет влияние на процессы и серверные системы, используемые ICANN (при выполнении функций IANA), VeriSign и NTIA. Например, объем данных в базе, которая используется для хранения контактной информации об администраторах

[11] Конечно, 300 бит в секунду является нереально низким значением, и более реалистичная скорость позволит передавать зону быстрее. Таким образом, использование значения 300 бит в секунду можно рассматривать как наихудший случай.

ДВУ, скорее всего, существенно вырастет, а процессы, используемые для рассмотрения запросов в каждой из организаций, участвующих в управлении корневой зоной, скорее всего, потребуется изменить с учетом увеличения нагрузки, связанной с повседневными модификациями корневой зоны. Однако все организации, принимающие участие в управлении корневой зоной, выразили намерение скорректировать свои ресурсы для удовлетворения растущих требований. Таким образом, на первый план выходит обнаружение возросших нагрузок до того, как они приведут к возникновению проблемы, и содействие корректировке ресурсов. По этой причине областями, в которых необходимо приложить дополнительные усилия, являются мониторинг системы управления корневой зоной в точках, являющихся ее потенциальными узкими местами, а также определение пороговых значений, сигнализирующих о возникновении проблемной области.

Резюме

Известно, что предсказание будущего является в определенной степени проблематичным. Однако в случае прогнозирования последствий масштабирования корневой зоны, представляется вероятным следующее: если предположить, что исторические тенденции развития событий не изменятся непредвиденным образом, ожидаемый рост с запасом находится в пределах возможностей адаптации системы к этому росту.

В случае IPv6 почти 70% доменов верхнего уровня, а также 8 из 13 корневых серверов уже выполнили развертывание IPv6. Маловероятно, что переход в обоих случаях к 100% приведет к каким-либо отрицательным последствиям (за исключением возможных задержек для конечных пользователей в связи с превышением времени ожидания из-за того, что инфраструктура IPv6 еще не достигла такого же уровня, что и инфраструктура IPv4).

В случае DNSSEC, хотя добавятся новые записи DS по мере подписания своих зон все большим числом ДВУ, маловероятно, что это приведет к каким-либо заметным изменениям в корневой зоне, за исключением того, что корневая зона будет расширяться с интенсивностью, (главным образом) связанной с количеством новых ДВУ.

И наконец, добавление новых ДВУ может оказать максимальное влияние, однако с учетом прогнозируемого предела менее 1000 новых ДВУ в год маловероятно, что этот рост приведет к каким-либо нарушениям работы при условии, что корректировка систем и процессов будет осуществляться в рамках обычной функциональной модернизации.

Заключение

По мере продолжения роста и развития DNS с целью удовлетворения новых требований, критически важным является обеспечение того, чтобы эти изменения не оказали отрицательного влияния на стабильность DNS. В исполнение

резолюции Правления ICANN 2009-02-03-04 было проведено два исследования для анализа последствий добавления IPv6, DNSSEC, ИДИ и новых рДВУ в корневую зону DNS. Исследование корневого сервера «L» продемонстрировало, что по крайней мере один корневой сервер может без труда справиться как с развертыванием новых технологий, так и с увеличением количества ДВУ на несколько порядков, даже по сравнению с ожиданиями в отношении возможности обработки заявок ICANN в обозримом будущем. В исследовании КМКС высказано предположение, что абсолютные количества не имеют такого важного значения, как интенсивность изменений и способы модификации различных процессов и серверных систем для управления корневой зоной с целью учета этих изменений.

Однако в период с принятия резолюции 2009-02-03-04 до настоящего времени развертывание новых технологий продолжалось, следовательно, можно использовать эмпирические данные для подтверждения правильности результатов обоих исследований. Развертывание IPv6 в корневой зоне, начатое в 2004 г., не оказало существенного вредного влияния. Аналогичным образом, введение ИДИ в корневую зону в 2007 г. не стало событием с точки зрения стабильности DNS, а развертывание DNSSEC в корневой зоне, начатое в январе 2010 г., не привело к каким-либо заметным отрицательным последствиям.

В перспективе маловероятно, что дальнейшее добавление IPv6, DNSSEC и ИДИ окажет какое-либо отрицательное влияние на стабильность DNS, хотя необходимо аккуратно управлять сменой ключа для подписания ключей в корневой зоне, чтобы обеспечить настройку новой отметки о доверии для корневой зоны на определителях, осуществляющих проверку подлинности, до истечения срока действия старой отметки о доверии. Единственной неизвестной величиной остается количество новых ДВУ, вводимых в корневую зону.

Один из очевидных выводов в результате проведения исследований согласно резолюции Правления ICANN 2009-02-03-04 и обсуждений в связи с этими исследованиями заключается в необходимости усовершенствования как мониторинга систем корневой зоны, так и информационного взаимодействия между различными заинтересованными сторонами, принимающими участие в управлении корневой зоной. Хотя к настоящему времени модификация корневой зоны не оказала заметного отрицательного влияния, можно обоснованно утверждать, что без дополнительного мониторинга и усовершенствования информационного взаимодействия можно не заметить прохождение корневой зоной критически важного порога при масштабировании, что приведет к проблемам масштабирования, которые могут оказать влияние на стабильность DNS в целом. В предположении, что ежегодно будет добавляться не более 1000 новых ДВУ, а мониторинг и информационное взаимодействие между соответствующими заинтересованными сторонами будет улучшено, кажется очевидным, что корневая система сохранит свою стабильность по мере изменения для удовлетворения новых потребностей.