Руководство по закупочной деятельности в DNS для специалистов по государственным закупкам

Офис технического директора ICANN

Дэвид Хуберман (David Huberman)
OCTO-013
24 июля 2020 г.

ICANN

СОДЕРЖАНИЕ

Этот документ входит в состав серии документов OCTO. См. страницу публикаций OCTO - здесь приведен список документов по порядку. Вопросы или предложения по любому из этих документов отправляйте на адрес octo@icann.org.

1 Введение

Это руководство призвано помочь должностным лицам, которые занимаются государственными закупками, сделать правильный выбор при покупке доменных имен и закупках в системе доменных имен (DNS), чтобы обеспечить безопасность, стабильность и отказоустойчивость именования служб и узлов ваших государственных сетей. Для использования данного руководства не нужно быть специалистом по DNS. Оно написано понятным языком, чтобы способствовать вашему сотрудничеству как с ИТ-отделом, так и с поставщиками.

Настоящий документ публикуется Интернет-корпорацией по присвоению имен и номеров (ICANN). ICANN — некоммерческая общественная корпорация, которая от имени интернет-сообщества следит за технической координацией самого верхнего уровня системы доменных имен (DNS) в интернете, помогая обеспечивать ее безопасность, стабильность и отказоустойчивость.

В данном руководстве предлагаются полезные оперативные технологии и практические методы. Не все поставщики предоставляют полный спектр перечисленных нами услуг или технологий. Но чтобы вы смогли принять полностью обоснованное решение о закупках, необходимо узнать, какие из рекомендуемых нами технологий они поддерживают, а какие нет.

В этом руководстве рассматриваются три этапа получения и активации доменных имен:

- Выбор доменного имени
- Регистрация доменного имени
- Функционирование DNS: хостинг для вашего доменного имени

2 Выбор доменного имени

Доменные имена заканчиваются суффиксом. Вот некоторые примеры этих суффиксов: *.com*, *.gov*, *.uk* и *.asia*. В DNS более 1300 таких суффиксов, которые называются доменами верхнего уровня или *TLD*. При выборе доменного имени в первую очередь необходимо решить, какой именно TLD будет использоваться, будь то имя общего пользования, называемое *gTLD* (такие суффиксы с общим значением, как «.com» или «.asia»), или двухбуквенный национальный домен верхнего уровня, называемый *ccTLD*, который обозначает признанную территорию (такие суффиксы, как *.fr* для Франции или *.za* для ЮАР, где каждый суффикс соответствует коду территории из списка, приведенного в стандарте ISO-3166-2).[1]

Во многих случаях, в том числе для соблюдения установленных местных правил и политики, государственным структурам, возможно, придется использовать доменное имя в ccTLD своей страны (например, *go.jp* для органа государственной власти в Японии). Различные правительства управляют своими ccTLD по-разному. Мы рекомендуем вам

[1] Дополнительные сведения о стандарте ISO-3166-2 см. здесь: https://www.iso.org/iso-3166-country-codes.html. ICANN **не** назначает коды ISO-3166. Этим занимается Агентство по техническому обеспечению ISO-3166.

поговорить с оператором служб доменных имен своего правительства, расспросить его о действующей политике и ознакомиться с его функциональными возможностями, средствами безопасности и планами обеспечения бесперебойной деятельности (как описано ниже), чтобы сравнить со всеми остальными доступными вариантами TLD. Контактные данные администраторов каждого TLD, в том числе ccTLD, публикуются в каталоге по адресу https://www.iana.org/domains/root/db (чтобы перейти к контактным данным, нажмите ссылку на TLD).

У ICANN есть договор с каждым gTLD, в котором установлено множество правил. В частности, gTLD обязаны соблюдать условия подписанного ими соглашения с ICANN об администрировании доменного имени.[2] Эти условия возлагают на администраторов gTLD определенные обязательства по соблюдению технических требований и политики, которые направлены как на улучшение состояния экосистемы DNS, так и на защиту владельцев доменных имен. В отличие от этого ccTLD не заключают соглашений с ICANN. Все доступные владельцу доменного имени средства правовой защиты, по всей вероятности, будут зависеть от юрисдикции, в которой работает регистратура ccTLD.

Независимо от того, регистрируете ли вы доменное имя в ccTLD или в TLD общего пользования, TLD может предложить четыре функции, которые мы считаем важными: поддержка DNSSEC, поддержка IPv6, реализация блокировки на стороне регистратуры в том или ином виде и репутация TLD.

2.1 Поддержка DNSSEC

Пользователи лучше защищены, если доменные имена криптографически подписаны владельцем доменного имени, то есть вашей организацией. Ваша организация может использовать цифровую подпись для своих доменных имен с помощью технологии под названием «Расширения безопасности системы доменных имен» (DNSSEC). Документ ICANN «DNSSEC: защита DNS» содержит более подробную информацию о важности DNSSEC.[3]

Чтобы подписать домен, необходимо выбрать TLD, который поддерживает технологию *подписи DNSSEC*. К счастью, большинство TLD (в том числе все TLD общего пользования) поддерживает DNSSEC. Однако, если поддержка DNSSEC не указана в списке доступных услуг выбранного TLD, вам следует узнать о текущей или планируемой поддержке этой функции. Следует признать, что выяснить, насколько хорошо TLD поддерживает DNSSEC, не всегда просто. Некоторые TLD публикуют эту информацию на своем сайте, а другие нет. Возможно, вам удастся найти эту информацию в интернете, или даже придется написать электронное письмо или позвонить им, чтобы поговорить об этом.

[2] Есть несколько версий соглашения с ICANN об администрировании домена верхнего уровня, и разными TLD подписаны разные версии. Действующая редакция называется «базовым соглашением об администрировании домена верхнего уровня 2017 года» и находится по адресу https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html

[3] См. https://www.icann.org/en/system/files/files/octo-006-en.pdf

2.2 Поддержка IPv6

Компьютеры в интернете используют адреса интернет-протокола (IP-адреса), чтобы другие вычислительные устройства могли их идентифицировать. Есть два вида IP-адресов: IPv4 и IPv6. IPv4-адреса являются наиболее распространенным видом IP-адресов. IPv6 — новый вид IP-адреса, разработанный для содействия дальнейшему росту интернета по мере добавления новых устройств.

Поскольку некоторые правительства требуют, чтобы инфраструктура интернета поддерживала адресацию как IPv4, так и IPv6, уточните у оператора TLD, поддерживаются ли для ваших DNS-серверов одновременно адреса IPv4 и IPv6. В частности, оператор TLD должен поддерживать наличие у вас авторитативных DNS-серверов имен с адресами IPv6. Если это так и ваш оператор TLD не поддерживает IPv6, мир не сможет получить доступ к сайтам в вашем домене.

2.3 Блокировка на стороне регистратуры

Другое важное соображение при выборе TLD — спросить у оператора TLD, поддерживает ли он функцию, называемую *блокировка на стороне регистратуры*.

Оператор TLD управляет «регистратурой», которая содержит все домены второго уровня, например, example.tld, внутри TLD.[4] Блокировка на стороне регистратуры позволяет владельцам доменных имен, которых также называют владельцами доменов, давать указание оператору TLD «заблокировать» доменное имя, точно так же, как вы запираете двери своего автомобиля. Когда ваш домен заблокирован, никто не может его изменить, удалить или передать другому владельцу домена без процедуры авторизации, которую вы определили вместе с оператором TLD. Однако обратите внимание, что нет отраслевых стандартов реализации блокировки на стороне регистратуры, поэтому вам следует выяснить у оператора TLD, предлагает ли он блокировку на стороне регистратуры, и если да, то как она работает.

В целом, мы считаем, что лучший процесс авторизации изменений включает «внешнюю» авторизацию, когда все стороны не полагаются на интернет-ориентированное общение, а вместо этого используют телефонные звонки или другой канал, в который злоумышленникам трудно проникнуть. Основные параметры доменного имени, как правило, меняются очень редко, поэтому приемлем более медленный процесс, такой как внешняя авторизация. В то же время, вероятно, стоит убедиться, что у вашего оператора TLD имеется четко прописанная процедура передачи разрешения проблем на более высокий уровень в еще более редком случае, когда какие-то данные DNS необходимо изменить в экстренном порядке.

Мы настоятельно рекомендуем всем владельцам доменов использовать TLD, поддерживающие блокировку на стороне регистратуры, поскольку это предотвращает известные атаки, которые могут поставить под угрозу целые домены.

[4] По непонятной причине оператор TLD также может называться регистратурой

2.4 Репутация

И наконец, прежде чем выбрать TLD, узнайте, какая у него репутация. По данным компании Spamhaus,[5] которая специализируется на борьбе со злоупотреблениями, TLD имеет плохую репутацию, если слишком большая доля зарегистрированных в нем доменных имен связана с такими действиями, как рассылка спама и вредоносного ПО. Хотя в любом TLD всегда будут регистрироваться вредоносные доменные имена, такие компании, как Spamhaus, оценивают портфели имен TLD в целом, чтобы определить «недобросовестность» или «добросовестность» TLD.

Важно выбрать такой TLD, где нет значительного количества злонамеренных регистраций. Когда у TLD плохая репутация в техническом сообществе, он может быть заблокирован интернет-провайдерами (ISP) и операторами корпоративных сетей. Если используемый вами TLD имеет плохую репутацию, вы не сможете, к примеру, отправлять электронную почту со своего домена, поскольку многие почтовые серверы автоматически настроены на блокировку электронной почты, которая поступает из доменов, включенных в черные списки.

Существует множество компаний, специализирующихся на борьбе с злоупотреблениями, которые публикуют рейтинги репутации TLD, в том числе Spamhaus и SURBL.[6]

3 Выбор регистратора доменного имени

После того как вы выбрали TLD для своего учреждения, вы регистрируете в нем доменное имя. В некоторых ccTLD можно регистрировать доменные имена напрямую через оператора TLD. Однако во многих ccTLD и в большинстве gTLD доменное имя регистрируется через «регистратора» доменных имен.[7] В данном разделе перечислены некоторые критерии, которые мы предлагаем принять во внимание при выборе потенциального регистратора доменных имен.

3.1 Аккредитация

ICANN предлагает регистраторам официальную аккредитацию. Успешное получение и сохранение аккредитации означает, что регистратор продемонстрировал свое соответствие всем техническим, эксплуатационным и финансовым критериям, необходимым для получения статуса компании-регистратора.[8] Важно отметить, что регистратор обязан соблюдать условия соглашения об аккредитации регистратора,[9] в котором предусмотрено множество средств защиты владельцев доменных имен.

5 См. https://www.spamhaus.org/

6 См. http://www.surbl.org/

7 Можно считать разделение на регистратуры и регистраторов аналогичным разделению оптовых и розничных продаж. То есть точно так же, как люди покупают товары у розничных продавцов, которые получают их от оптовиков, владельцы доменов покупают доменные имена у регистраторов, которые получают свои товарные запасы от регистратур.

8 Описание аккредитационных требований представлено здесь: https://www.icann.org/resources/pages/policy-statement-2012-02-25-ru#IIA

9 Действующая редакция RAA опубликована здесь: https://www.icann.org/resources/pages/registrars/registrars-en

При регистрации доменного имени в gTLD убедитесь, что вы выбрали регистратора, аккредитованного ICANN. Список аккредитованных регистраторов находится на сайте ICANN.[10] Соглашение, которое регистраторы заключают с ICANN, также позволяет им сотрудничать с «реселлерами». Это сторонние компании, предлагающие услуги по регистрации доменных имен от имени регистратора. Однако при покупке доменов с высокой ценностью мы рекомендуем по возможности работать напрямую с аккредитованными регистраторами, поскольку это сокращает число участвующих сторон, если возникает необходимость решения неотложной проблемы.

При регистрации доменного имени в gTLD убедитесь, что вы обратились к регистратору или реселлеру, который уполномочен регистратурой соответствующего ccTLD.

3.2 Основные средства обеспечения безопасности

Любой выбранный вами регистратор доменных имен должен поддерживать надежные пароли (как правило, это длинные строки, в составе которых есть хотя бы одна буква верхнего регистра, одна буква нижнего регистра и хотя бы один символ) и предлагать пользователям, заходящим в свои учетные записи на портале, многофакторную аутентификацию (пароль плюс некоторый токен безопасности, который часто представляет собой SMS-код, отправляемый на мобильный телефон).

Вам также следует обратиться к своему регистратору или реселлеру и удостовериться, что канал связи с сайтом, где размещен портал для доступа к учетным записям клиентов, шифруется с использованием HTTPS. Это помогает обеспечить конфиденциальность обмена электронными сообщениями между вашим ИТ-персоналом и регистратором/реселлером.

3.3 Поддержка DNSSEC

Если вы приложили усилия и убедились, что ваша регистратура поддерживает DNSSEC, важно выбрать регистратора, который позволит передавать необходимые данные, относящиеся к DNSSEC, и, если вы не управляете своими зонами напрямую, подписать ваши зоны с помощью DNSSEC. Регистраторы, как правило, должны публиковать информацию о поддержке служб DNSSEC на своем сайте. Возможно, вы также захотите, чтобы ваш технический персонал обсудил с регистратором уровень поддержки DNSSEC, чтобы обеспечить соблюдение ваших технических требований.

3.4 Поддержка IPv6

Регистратор доменных имен должен поддерживать использование как адресов IPv4, так и адресов IPv6, то есть позволять вам управлять адресными записями ресурсов («A» и «AAAA») для всех устройств, которым вы хотите присвоить имена в рамках своего доменного имени.

[10] См. https://www.icann.org/registrar-reports/accreditation-qualified-list.html

3.5 Экспорт данных

При ориентации на долгосрочную перспективу вы не захотите быть навсегда привязанными к одному регистратору доменных имен. Могут измениться ваши технологические потребности, может снизиться качество услуг регистратора или в будущем может произойти что-то еще, что побудит вас перенести свои доменные имена к другому регистратору. В связи с этим было бы полезно, чтобы регистратор позволял вам «экспортировать данные вашей зоны», то есть он позволял вам загружать все данные DNS, связанные с вашими доменными именами. Это дает вам контроль над данными DNS своих доменов и позволяет ИТ-персоналу быстро перейти на обслуживание к новому регистратору.

3.6 Репутация

Любой выбранный вами регистратор доменных имен должен иметь как хорошую репутацию в области борьбы со злоупотреблениями, так и подтвержденный опыт сотрудничества с национальными и международными правоохранительными агентствами при получении сообщений о неправильном использовании DNS. Например, вы должны убедиться, что у регистратора есть солидная программа борьбы с мошенничеством, которая позволяет обнаруживать и аннулировать регистрации доменных имен, связанные с использованием украденных данных кредитных карт.

4 Функционирование DNS: сторонний хостинг для вашего доменного имени

Зарегистрированное доменное имя должно быть где-то размещено. Его можно разместить в ИТ-отделе вашего государственного органа, но может появиться возможность или даже необходимость выбора стороннего поставщика для размещения ваших доменных имен в его дата-центрах. Такой хостинг может быть предложен в составе пакета услуг, который вы покупаете у ИТ-провайдера. Данный раздел призван помочь вам выбрать стороннего поставщика и в нем перечислен ряд аспектов, которые мы считаем важными.

4.1 Управление доменными именами

Важно, чтобы у вас была возможность быстро и без труда создавать поддомены. Поддомен — это доменное имя, которое имеет вид *mail.department.za*, *elections.government.co.jp* или аналогичный. Вам следует выяснить, насколько легким будет создание, изменение и удаление поддоменов, особенно в массовом порядке. Также важно, чтобы вы могли создавать современные типы записей DNS, например, тип записи TLS-аутентификации (TLSA), который используется технологией безопасности под названием «DNS-аутентификация именованных объектов» (DANE).

4.2 Безопасность деятельности

Одним из наиболее важных соображений при покупке услуг DNS является безопасность. Очень важно, чтобы ваша организация при любых обстоятельствах *сохраняла контроль* над всеми своими доменными именами и размещенных на них службами. Лучший способ

сохранить этот контроль — всегда сотрудничать с такими поставщиками (от регистраторов доменных имен до ИТ-провайдеров), которые обладают высокой культурой и приверженностью безопасности. При потере вами контроля над частью своих технологий DNS, атаки могут происходить очень быстро и возможна утечка данных.

Что касается сторонних хостинг-провайдеров, мы отметим три элемента безопасности, которые имеют решающее значение для надежного обеспечения безопасности:

- Они должны предлагать многофакторную аутентификацию для входа в учетную запись. Если доступ к технологиям осуществляется через один фактор (например, пароль), он не является безопасным.
- У провайдера должны быть опубликованные комплексные методы и политика обеспечения безопасности.
- Провайдер должен также предлагать углубленный мониторинг безопасности элементов инфраструктуры и данных DNS. Такой мониторинг должен выполняться регулярно, чтобы гарантировать быстрое обнаружение любых изменений, внесенных злоумышленником. У провайдера должна быть многоуровневая система оповещений для уведомления технического персонала при обнаружении нештатных действий.

Как правило, также важно поинтересоваться, поддерживается ли *BCP 38.*[11] BCP 38 — это документ, где определены методы работы, которых должны придерживаться провайдеры для сокращения количества мошеннических действий при маршрутизации в интернете. Все сетевые провайдеры должны поддерживать BCP 38. В некоторых исключительных случаях могут существовать причины, по которым невозможно соблюдать BCP 38, но в среде типичных организаций, предлагающих услуги хостинга доменов, такие случаи — необычное явление, и вам следует получить подробное объяснение.

4.3 Авторитативная DNS-служба

Авторитативная DNS-служба — это способ сообщить миру, что ваше доменное имя разрешается в конкретные IP-адреса, какой почтовый сервер вы используете для входящей почты, как устроено пространство имен вашей организации и т. д. Планируете ли вы установить собственные авторитативные DNS-серверы или собираетесь платить стороннему провайдеру за размещение авторитативных DNS-серверов от вашего имени, следует помнить о нескольких аспектах:

- Лучше всего иметь несколько отдельных авторитативных DNS-серверов в разделенных географически и топологически сетях.
- Убедитесь, что все службы хостинга DNS-серверов полностью поддерживают DNSSEC, включая загрузку записей DNSKEY и DS вашему регистратору доменных имен.
- Убедитесь, что есть хорошая поддержка крупномасштабного добавления, изменения или удаления данных DNS, включая записи ресурсов и поддомены.
- Изучите меры защиты от распределенных атак типа «отказ в обслуживании», независимо от того, собираетесь ли вы использовать собственные DNS-серверы или настроить их у стороннего провайдера.

[11] См. https://datatracker.ietf.org/doc/bcp38/

4.4 Поддержка IPv6

Возрастает важность поддержки сторонним хостинг-провайдером протокола IPv6 в программном обеспечении и службах. Региональные интернет-регистратуры (RIR), которые занимаются распределением IP-адресов на верхнем уровне, подготовили множество материалов, чтобы помочь вам принимать правильные решения о закупках, связанных со службами, где используются IP-адреса. В том числе:

- AFRINIC, RIR Африки, составила руководство по IPv6 для органов государственной власти.[12]
- ARIN, RIR Северной Америки и некоторых стран Карибского бассейна, подготовила 6-минутный видеоролик с объяснением того, что такое IPv6 и почему он важен.[13]
- LACNIC, RIR Латинской Америки, опубликовала руководство по 12-этапному внедрению протокола IPv6 для правительств и предприятий.[14]
- RIPE NCC, RIR Европы и части Передней Азии, опубликовала руководство, в котором сформулированы требования, предъявляемые протоколом IPv6 к оборудованию ИКТ.[15]

5 Резюме

В этом руководстве рассмотрено очень много вопросов. Опять-таки, не все поставщики смогут предложить все перечисленные здесь услуги, которые мы считаем важными. Но основные мысли, которые мы надеемся до вас донести, таковы:

- Безопасность важна, и она намного шире, чем просто правильно выбранный пароль.
- Поддержка DNSSEC и поддержка IPv6 должны входить в число основополагающих требований.
- Компании, с которыми вы сотрудничаете, должны стремиться сохранять хорошую репутацию в области противодействия злоупотреблениям и рассмотрения жалоб на злоупотребления.

12 См. https://afrinic.net/guidebook-gov-ipv6
13 См. https://youtu.be/bkLs5_geTM4
14 См. https://www.lacnic.net/innovaportal/file/3635/1/10-12-steps-government-ipv6-v3.pdf
15 См. https://www.ripe.net/publications/docs/ripe-554

Приложение: Контрольный список закупок

Выбор регистратуры TLD

- ❑ Поддерживает DNSSEC

  Зарегистрированные в TLD доменные имена могут быть подписаны с использованием DNSSEC

- ❑ Поддерживает как IPv4, так и IPv6

  Записи DNS-серверов TLD могут публиковаться как с адресами IPv4, так и с адресами IPv6

- ❑ Предлагает блокировку на стороне регистратуры

  Имеет процесс блокировки записей и требует внешней авторизации для внесения изменений в заблокированные записи

- ❑ Имеет хорошую репутацию

  TLD активно борется с доменными именами, которые зарегистрированы в этом TLD для злоупотреблений

Выбор регистратора доменного имени

- ❑ Является аккредитованным или уполномоченным регистратором

  Если gTLD, то аккредитован ICANN, а если ccTLD, то уполномочен предлагать домены

- ❑ Практикует хорошую кибер-гигиену

  Требует многофакторной аутентификации для входа в учетную запись пользователя и использует HTTPS на веб-страницах

- ❑ Поддерживает DNSSEC

  Доменные имена могут быть подписаны с использованием DNSSEC

- ❑ Позволяет размещать доменные имена у третьих лиц

  Поддерживает только регистрацию доменных имен и не заставляет вас размещать доменное имя на своих веб-серверах

- ❑ Позволяет экспортировать данные

  Данные DNS могут быть экспортированы вашим ИТ-персоналом, чтобы вы могли без труда передать их новому регистратору

- ❑ Поддерживает как адреса IPv4, так и адреса IPv6

  Записи DNS-серверов могут публиковаться как с адресами IPv4, так и с адресами IPv6

- ❑ Имеет хорошую репутацию

  Активно предотвращает, выявляет и сдерживает злоупотребления, а также реагирует на жалобы

Выбор стороннего хостинг-провайдера

- ❑ Поддерживает как массовое управление поддоменами, так и современные типы записей DNS

  Можно добавлять, изменять или удалять поддомены в массовом порядке и добавлять записи ресурсов, такие как TLSA

- ❑ Имеет средства обеспечения безопасности

  Многофакторная аутентификация при входе пользователей в систему, опубликованные практические методы и политика обеспечения безопасности, упреждающий мониторинг данных DNS и поддержка BCP38

- ❑ Поддержка авторитативных DNS-служб

  Географически разнесенные DNS-серверы, хорошая защита от атак и другие средства

- ❑ Поддерживает как адреса IPv4, так и адреса IPv6

  При доступе к серверам провайдера и обновлении DNS-серверов поддерживается как IPv4, так и IPv6