



Проект Руководства для кандидата, третье версия

Модуль 5

Все материалы, содержащиеся в черновой версии Руководства кандидата, представлены для публичного комментирования. Обратите внимание, что это только черновик, предназначенный для обсуждения. Потенциальным кандидатам не следует полагаться на точность описываемых деталей новой программы gTLD, поскольку программа все еще подвергается обсуждению и пересмотру.

Данный документ переведен с английского языка в целях расширения аудитории его читателей..

Несмотря на усилия, предпринятые некоммерческой организацией ICANN в отношении проверки точности перевода, единственной официальной версией данного документа, имеющей силу, является англоязычная версия, поскольку английский является рабочим языком ICANN.

2 октябрь 2009

Модуль 5

Переход к передаче

В этом модуле описываются заключительные действия, которые необходимо предпринять кандидату, включая оформление соглашения о регистрации с ICANN и подготовку передачи новой строки gTLD в корневую зону.

5.1 Соглашение о регистрации

Все кандидаты, успешно прошедшие процесс оценки, включая (при необходимости) процессы разрешения споров и разногласий в отношении строк, должны заключить с ICANN соглашение о регистрации, чтобы перейти к передаче.

Черновой вариант соглашения о регистрации содержится в приложении к данному модулю. Все кандидаты, успешно прошедшие процесс оценки, должны заключить соглашение. Важно отметить, что соглашение, о котором идет речь выше, не выражает официальную позицию ICANN и не было утверждено Советом директоров ICANN. Данное соглашение представлено в черновом варианте для ознакомления и обсуждения сообществом, а также в целях повышения его эффективности как средства создания условий для увеличения конкуренции и расширения потребительского выбора в стабильной и защищенной DNS.

Перед тем, как заключить с кандидатом соглашение о регистрации, ICANN может выполнить предконтрактную проверку. Чтобы убедиться в том, что кандидат обладает надлежащей правосубъектностью, ICANN оставляет за собой право потребовать от кандидата предоставить обновленную документацию и информацию перед заключением соглашения о регистрации.

Перед или одновременно с оформлением соглашения о регистрации кандидат должен также предоставить документально подтвержденное доказательство своей способности обеспечить финансирование основных операций реестра для будущих владельцев регистрации на период от трех до пяти лет, в случае банкротства реестра, невыполнения

денежных обязательств, или пока не будет назначен следующий оператор. Для выполнения данного обязательства требуется предоставить финансовый инструментарий, как описано в разделе «Критерии оценки».

5.2 Проверка перед передачей

В качестве предварительного условия для передачи строки в корневую зону каждый кандидат будет должен выполнить техническую проверку. Данная проверка перед передачей должна быть завершена в течение периода времени, указанного в соглашении о регистрации.

Цель технической проверки перед передачей состоит в том, чтобы убедиться, что кандидат выполнил свое обязательство по запуску реестра в соответствии с техническими и рабочими критериями, описанными в Модуле 2.

Эта проверка также направлена на то, чтобы убедиться в способности кандидата обеспечить стабильную и безопасную работу gTLD. Все кандидаты будут тестироваться с присвоением оценок «прошел»/«не прошел» на основании следующих требований.

В рамках проверки будут протестированы как операционная инфраструктура сервера DNS, так и функционирование реестра. В большинстве случаев кандидат самостоятельно выполнит все этапы проверки, в соответствии с инструкциями, и предоставит документированные результаты в ICANN для подтверждения удовлетворительных рабочих показателей. По своему усмотрению, ICANN может выполнить проверку ряда аспектов этой документации на месте (в пункте предоставления услуг реестра).

5.2.1 Порядок проверки

Кандидат может инициировать проверку перед передачей, отправив в ICANN специальную форму и сопроводительные документы, содержащие следующую информацию:

- все имена и адреса IPv4/IPv6 сервера имен, которые будут использоваться при обслуживании данных нового TLD;

- при использовании резервирования – список имен и адресов unicast IPv4/IPv6, используемых для идентификации каждого отдельного сервера в наборах резервирования;
- при поддержке IDN – полный список таблиц IDN, используемых в системе реестра;
- во время проверки должна быть подписана зона нового TLD; кроме того, в документации для ICANN должен быть указан действительный набор ключей для использования во время проверки, а также определение стратегии безопасности DNSSEC (DPS);
- подписанное соглашение с агентом по условному депонированию;
- документированные результаты самопроверки, как описано ниже для каждого элемента проверки.

ICANN проанализирует поданный материал и, в некоторых случаях, выполнит дополнительные проверки. По завершении данных этапов проверки ICANN создаст отчет по результатам проверки и представит его кандидату.

В данном отчете будут перечислены все запросы на разъяснение, запросы на предоставление дополнительной информации или общие запросы ICANN, возникшие в процессе анализа документации.

Если кандидат удовлетворяет всем требованиям проверки перед передачей, он может подать запрос на передачу указанной в заявке строки gTLD. Все передачи в корневую зону должны быть утверждены Советом директоров ICANN.

Если кандидат не выполнил проверку перед передачей в течение срока, указанного в соглашении о регистрации, ICANN оставляет за собой право аннулировать соглашение о регистрации.

5.2.2 Элементы проверки: Инфраструктура DNS

Первый набор элементов проверки связан с инфраструктурой DNS нового gTLD.

Требования к производительности системы.

Подлежащая проверке инфраструктура DNS объединяет в себе полный набор инфраструктуры сервера и сети, который будет использоваться потенциальным поставщиком услуг DNS для новых gTLD в Интернете. В документации, предоставленной кандидатом, должны быть представлены результаты проверки производительности системы с указанием рабочей мощности сети и сервера, а также предварительного расчета ожидаемой мощности для обеспечения стабильной работы и защиты от распределенных атак типа отказ в обслуживании (DDoS).

Документированные результаты самопроверки должны содержать данные по нагрузке, времени запаздывания и доступности сети.

Показатели нагрузки должны быть представлены в виде таблицы и соответствующего графика с указанием процентного отношения обработанных запросов к возрастающему количеству запросов от локального сервера в секунду, генерируемых имитаторами нагрузки. Таблица должна содержать не менее 20 значений и нагрузок, что составит до 10% потери запросов. Действительные ответы должны содержать данные зоны или быть в форме ответов NXDOMAIN или NODATA.

Время запаздывания выражается в миллисекундах, в соответствии с измерениями зондов DNS, расположенных за пределами граничных маршрутизаторов физической сети, в которой размещены серверы.

Доступность будет документально подтверждена путем предоставления информации по соглашениям о передаче и обмене трафиком для размещений сервера DNS, с указанием номеров AS поставщиков услуг передачи или узлов партнера в каждой точке подключения, а также доступной пропускной способности в этих точках.

Поддержка TCP. Служба передачи TCP для запросов и ответов DNS должна быть включена, при этом должен

быть обеспечен необходимый режим мощности для ожидаемой нагрузки. ICANN выполнит проверку отчета по рабочей мощности, предоставленного кандидатом, а также проведет тестирование доступности TCP и возможности транзакции для каждого из сервера имен, перечисленных кандидатом. В случае использования резервирования будет протестирован каждый отдельный сервер в каждом наборе резервирования. Документированные результаты самопроверки должны содержать данные по нагрузке, времени запаздывания и доступности внешней сети.

Показатели нагрузки должны быть представлены в виде таблицы и соответствующего графика с указанием процентного отношения обработанных запросов к возрастающему количеству запросов от локального сервера в секунду, генерируемых имитаторами нагрузки. Таблица должна содержать не менее 20 значений и нагрузок, что составит до 10% потери запросов. Действительные ответы должны содержать данные зоны или быть в форме ответов NXDOMAIN или NODATA.

Время запаздывания выражается в миллисекундах, в соответствии с измерениями зондов DNS, расположенных за пределами граничных маршрутизаторов физической сети, в которой размещены серверы, с точки зрения топологии сети.

Доступность будет документально подтверждена путем предоставления записей запросов DNS на базе протокола TCP от узлов, расположенных вне сети, в которой размещены серверы. Эти могут быть местоположения, использованные ранее для измерения времени запаздывания.

Поддержка IPv6. Кандидат должен обеспечить работу службы IPv6 в рамках своей инфраструктуры DNS. ICANN выполнит проверку документации, предоставленной кандидатом, а также протестирует доступность IPv6 из различных точек Интернета. Также будут проверены возможности транзакции DNS на базе IPv6 для всех серверов имен с объявленными адресами IPv6. В случае использования резервирования будет протестирован каждый отдельный сервер в каждом наборе резервирования.

Документированные результаты самопроверки должны

содержать данные по нагрузке, времени запаздывания и доступности внешней сети.

Для набора серверов DNS, поддерживающих IPv6, показатели нагрузки должны быть представлены в виде таблицы и соответствующего графика с указанием процентного отношения обработанных запросов к возрастающему количеству запросов от локального сервера в секунду, генерируемых имитаторами нагрузки. Таблица должна содержать не менее 20 значений и нагрузок, что составит до 10% потери запросов. Действительные ответы должны содержать данные зоны или быть в форме ответов NXDOMAIN или NODATA.

Время запаздывания выражается в миллисекундах, в соответствии с измерениями зондов DNS, расположенных за пределами граничных маршрутизаторов физической сети, в которой размещены серверы.

Доступность будет документально подтверждена путем предоставления записей запросов DNS на базе протокола IPv6 от узлов, расположенных вне сети, в которой размещены серверы. Кроме того, кандидат должен предоставить подробную информацию по соглашениям о передаче и обмене трафиком IPv6, включая список номеров AS, с помощью которых происходит обмен трафиком IPv6.

Поддержка DNSSEC. Кандидат должен продемонстрировать поддержку EDNS(0) в своей инфраструктуре сервера, способность возвращать правильные ресурсные записи DNSSEC, такие как DNSKEY, RRSIG и NSEC/NSEC3, для подписанной зоны, а также способность принимать и публиковать ресурсные записи DS от администраторов доменов второго уровня. ICANN выполнит проверку материалов, предоставленных кандидатом, в также протестирует доступность и возможности транзакции DNS для запросов DNS с использованием расширения протокола EDNS(0) по каждому серверу имени. В случае использования резервирования будет протестирован каждый отдельный сервер в каждом наборе резервирования.

Показатели нагрузки, времени запаздывания и доступности должны быть документально подтверждены, как указано выше для протокола ТСП.

5.2.3 Элементы проверки: Системы реестра

Как зафиксировано в соглашении о регистрации, общая система регистрации реестра должна поддерживать протокол EPP. Кроме того, помимо поддержки инфраструктуры DNS, реестр должен предоставлять услуги службы «Кто есть кто» через порт 43 и веб-интерфейс. В данном разделе подробно изложены требования для проверки этих систем реестра.

Производительность системы. Система реестра должна соответствовать требованиям к производительности, описанным в Спецификации 6 соглашения о регистрации, и ICANN потребует провести самопроверку на соответствие этим требованиям. ICANN выполнит проверку документации, предоставленной кандидатом, для подтверждения соответствия этим минимальным требованиям.

Поддержка службы «Кто есть кто». Кандидат должен обеспечить соответствие службы «Кто есть кто» прогнозируемой нагрузке. ICANN выполнит проверку доступности данных службы «Кто есть кто» через порт 43 и веб-интерфейс, а также выполнит проверку предоставленной документации по возможностям транзакции службы «Кто есть кто». ICANN выполнит проверку доступа к службе «Кто есть кто» (через порт 43 и через веб-интерфейс) удаленно из различных точек Интернета.

В документации по результатам самопроверки должно быть описано максимальное количество запросов в секунду, успешно обработанных через серверы 43 и веб-интерфейс, а также сведения о прогнозируемой нагрузке.

Кроме того, кандидат должен представить описание развернутых функций управления по обнаружению и снижению рисков интеллектуального анализа данных из базы данных «Кто есть кто».

Поддержка EPP. В рамках услуги общей регистрации кандидат должен предоставить поддержку EPP с учетом прогнозируемой нагрузки. ICANN проверит соблюдение соответствующих RFC (включая расширения EPP для DNSSEC). ICANN также выполнит проверку предоставленной кандидатом документации по возможностям транзакции EPP.

В данной документации должно быть указано максимальное количество транзакций в секунду для интерфейса EPP по 10 значениям, соответствующим размерам базы данных реестра – от 0 (пусто) до прогнозируемого размера после одного года работы реестра, как установлено кандидатом.

В документации также должны быть указаны меры, принятые для управления нагрузкой на начальных этапах работы реестра, напр., в период случайного присвоения.

Поддержка IPv6. ICANN проверит способность реестра оказывать поддержку регистраторам при добавлении, изменении или удалении записей IPv6, предоставленных владельцами регистрации. Если реестр поддерживает доступ EPP по протоколу IPv6, ICANN протестирует данный механизм удаленно из различных точек Интернета.

Поддержка DNSSEC support. ICANN проверит способность реестра оказывать поддержку регистраторам при добавлении, изменении и удалении ресурсных записей DNSSEC, а также выполнит проверку основных механизмов управления реестра. Кроме того, будет проверено взаимодействие каналов безопасной связи кандидата с IANA для обмена сертификатами «точки доверия».

На данном этапе также проверяется документ по технологии и стратегии (также известный как «определение стратегии безопасности DNSSEC (DPS)»), в котором описано хранение, использование и доступ к основным материалам с помощью собственных ключей и сертификатов «точки доверия» владельцев регистрации.

Поддержка IDN. ICANN проверит все таблицы IDN table, используемые в системе реестра. Таблицы должны

соответствовать правилам, изложенным в документе <http://iana.org/procedures/idn-repository.html>.

Требования в отношении службы «Кто есть кто» IDN находятся в процессе разработки. После завершения разработки данных требований потенциальные реестры должны будут продемонстрировать соответствие опубликованным требованиям к службе «Кто есть кто» IDN в рамках проверки перед передачей.

Условное резервирование. Будут проверены предоставленные кандидатом примеры резервирования фиктивных данных (один пример полного и один пример инкрементного резервирования), правильность типа и форматирования содержимого. Особое внимание будет уделено соглашению с поставщиком услуг по условному резервированию для гарантии того, что резервированные данные могут быть восстановлены, и реестр восстановлен в точке, откуда, при необходимости, он сможет ответить на запросы DNS и службы «Кто есть кто» (через порт 43 и веб-интерфейс).

5.3 Процесс передачи

После получения уведомления об успешном завершении проверки перед передачей ICANN кандидаты могут начать процесс передачи нового gTLD в базу данных корневых зон. Информацию о процессе передачи см. на странице <http://iana.org/domains/root/>.

5.4 Текущие операции

Кандидат, успешно выполнивший передачу gTLD, получает статус «оператора реестра». Принимая на себя роль оператора системы доменных имен Интернета, кандидат также принимает на себя ряд важных обязательств. ICANN будет контролировать выполнение обязательств операторами новых gTLD, в соответствии с положениями соглашения о регистрации; при этом важно, чтобы все кандидаты понимали свои обязанности.

5.4.1 Обязанности оператора реестра

В соглашении о регистрации определены обязательства операторов реестра gTLD. Нарушение обязательств оператора реестра может привести к

соответствующим действиям ICANN, вплоть до аннулирования соглашения о регистрации. Потенциальным кандидатам рекомендуется ознакомиться со следующим кратким описанием некоторых из данных обязательств.

Помните, что данный перечень не является исчерпывающим и представлен только для общего ознакомления кандидатов с обязательствами оператора реестра. Полный утвержденный перечень обязательств содержится в черновом варианте соглашения о регистрации.

Оператор реестра обязан соответствовать следующим требованиям.

Обеспечение стабильной и безопасной работы TLD.

Оператор реестра несет полную ответственность за все операции TLD. Как указано в RFC 1591:

«Уполномоченный диспетчер домена должен обеспечить удовлетворительную работу службы DNS. А именно: фактическое управление назначением доменных имен, передача субдоменов и управление серверами имен должны осуществляться технически компетентно. Сюда входит предоставление рекомендаций по состоянию домена диспетчеру центрального IR¹ (в случае доменов высшего уровня) или других доменов высокого уровня; своевременное реагирование на запросы; а также обеспечение четкой, надежной и отказоустойчивой работы базы данных». Оператор реестра должен соблюдать соответствующие технические стандарты в виде RFC и других указаний. Кроме того, оператор реестра должен соответствовать спецификациям характеристик в таких областях, как время простоя системы и время реакции системы (см. Спецификацию 6 чернового варианта соглашения о регистрации).

Соблюдение стратегии общего согласия и временных политик. Операторы реестров gTLD обязаны соблюдать стратегию общего согласия. Стратегия общего согласия может затрагивать такие темы, как проблемы, влияющие на функциональную совместимость DNS, спецификации показателей и функций реестра,

¹ IR – первоначальное обозначение «Интернет-реестра», функции которого в настоящее время перешли к ICANN.

безопасность и стабильность базы данных, а также разрешение споров относительно регистрации доменных имен.

Для утверждения в качестве стратегии общего согласия, данная стратегия должна быть разработана Организацией поддержки общих имен (GNSO)² в соответствии с процедурой, описанной в Приложении А Устава ICANN.³ Процедура разработки стратегии, включающая в себя обсуждение и сотрудничество различных организаций, участвующих в процессе, а также возможность публичного комментирования, может занять довольно продолжительное время.

В качестве примеров стратегии общего согласия можно привести Политику передачи между регистраторами (регулирует передачу доменных имен между регистраторами) и Стратегию оценки услуг реестра (регулирует проверку безопасности и стабильности служб нового потенциального реестра, а также рассматривает вопросы конкуренции). Другие примеры можно найти на странице <http://www.icann.org/en/general/consensus-policies.htm>.

Операторы реестров gTLD обязаны соблюдать обе существующие стратегии общего согласия, а также все стратегии, которые будут разработаны в будущем. После официального утверждения стратегии общего согласия ICANN отправит операторам реестров уведомления с требованием внедрения новой стратегии и указанием даты вступления в силу.

Кроме того, Совет директоров ICANN может, в соответствующих обстоятельствах, разработать временную политику для обеспечения стабильности или безопасности услуг регистрации или DNS. В этом случае операторы реестров gTLD будут должны соблюдать данную временную политику в течение установленного периода времени.

Для получения дополнительной информации см. Спецификацию 1 чернового варианта соглашения о регистрации.

² <http://gns0.icann.org>

³ <http://www.icann.org/en/general/bylaws.htm#AnnexA>

Внедрение механизмов защиты прав. Оператор реестра должен соблюдать и внедрять решения, принятые в соответствии с Политикой разрешения споров после передачи торговой марки (Trademark Post-Delegation Dispute Resolution Policy, PDDRP). Кроме того, оператор реестра должен удовлетворять требованиям специальных механизмов защиты прав, разработанных и включенных в соглашение о регистрации (см. Спецификацию 7 чернового варианта соглашения).

Внедрение мер по защите географических имен новых gTLD. Все операторы реестров новых gTLD обязаны предоставить определенные минимальные средства защиты для имен стран и территорий, включая начальные требования к резервированию и все применимые правила и процедуры для выдачи данных имен. Операторам реестров настоятельно рекомендуется внедрить дополнительные средства защиты географических имен, помимо средств, перечисленных в соглашении, в соответствии с нуждами и интересами в каждом отдельном случае. (См. Спецификацию 5 чернового варианта соглашения).

Выплата периодических взносов ICANN. Помимо существующих расходов, связанных с осуществлением целей, изложенных в заявленной миссии ICANN, эти средства позволят предоставить необходимую поддержку новым gTLD, включая следующее: обеспечение соблюдения договорных требований, обмен информацией между реестрами, растущее количество аккредитаций регистраторов и другие меры по поддержке реестров. Взносы состоят из двух частей: фиксированного компонента (25 000 долларов в год) и, после того, как размер TLD превысит максимально допустимое значение, - переменного взноса, который рассчитывается на основе объема транзакций. См. Статью 6 чернового варианта соглашения.

Регулярное условное резервирование данных. Этот процесс играет важную роль для защиты владельцев регистраций и обеспечения непрерывности работы реестра в случаях, когда происходит системный сбой или потеря данных в реестре или какой-либо его части. (См. Спецификацию 2 чернового варианта соглашения о регистрации).

Своевременное предоставление ежемесячных отчетов. Оператор реестра должен предоставлять в ICANN ежемесячный отчет. В отчет входит статистика производительности за месяц, транзакции регистратора и другие данные. ICANN использует данный отчет для контроля за соблюдением требований, а также для расчета суммы сборов с регистраторов. (См. Спецификацию 3 чернового варианта соглашения о регистрации).

Предоставление услуг базы данных «Кто есть кто». Оператор реестра должен предоставить общедоступную службу «Кто есть кто» для зарегистрированных в TLD доменных имен. (См. Спецификацию 4 чернового варианта соглашения о регистрации).

Сотрудничество с регистраторами, аккредитованными ICANN. Оператор реестра разрабатывает Соглашение Реестр-Регистратор (RRA), в котором определены требования к регистраторам. Сюда входят определенные условия, указанные в соглашении о регистрации, а также дополнительные условия для конкретного TLD. Оператор реестра должен предоставить недискриминационный доступ к услугам реестра всем регистраторам, аккредитованным ICANN, с которыми заключено соглашение RRA и которые соответствуют установленным требованиям. Сюда также входит предварительное уведомление всех регистраторов о ценовых изменениях, в соответствии со сроками, определенными в соглашении. (См. Статью 2 чернового варианта соглашения о регистрации).

Создание службы контактов для сообщения о нарушениях. Оператор реестра должен создать на своем веб-сайте службу контактов для рассмотрения вопросов, требующих немедленного внимания, и своевременного реагирования на сообщения о нарушениях относительно всех имен, зарегистрированных в данном TLD через всех официальных регистраторов, включая торговых посредников. (См. Спецификацию 6 чернового варианта соглашения о регистрации).

Сотрудничество при проведении проверок соответствия требованиям. Чтобы обеспечить равные условия и согласованность операционной среды,

сотрудники ICANN выполняют периодические проверки для оценки соответствия условиям договора и решения любых связанных проблем. При выполнении таких проверок оператор реестра должен предоставить документы и информацию по запросу от ICANN. (См. Статью 2 чернового варианта соглашения о регистрации).

Обеспечение механизма для поддержания непрерывности процессов. При заключении соглашения оператор реестра должен продемонстрировать наличие механизма для поддержания непрерывности основных процессов реестра в течение трех (3) лет. Данное требование сохраняется в течение пяти (5) лет после передачи TLD; по истечении этих 5 лет оператор реестра больше не обязан обслуживать данный механизм для поддержания непрерывности процессов. (См. Спецификацию 8 чернового варианта соглашения о регистрации).

Соблюдение стратегий и процедур сообщества. Если в период подачи оператор реестра обозначил свою заявку как заявку от сообщества, соглашение о регистрации такого оператора будет содержать требования по соблюдению стратегий и процедур сообщества, указанных в заявке. При возникновении споров относительно соблюдения оператором реестра стратегий и процедур сообщества будет использоваться Процедура разрешения споров об ограничениях регистрации. (См. Статью 2 чернового варианта соглашения о регистрации).

5.4.2 Обязанности ICANN

ICANN продолжит предоставлять поддержку операторам реестра gTLD при запуске и управлении реестром. Представительные органы регистратуры gTLD ICANN осуществляют координацию операторов реестра gTLD и оказывают необходимую помощь на постоянной основе.

ICANN будет также выполнять проверки на соответствие операторов реестра своим договорным обязательствам и проводить анализ жалоб от сообщества по поводу несоблюдения оператором своих договорных обязательств.

Согласно Уставу ICANN, корпорация должна действовать открыто и прозрачно, а также

предоставлять равные права операторам реестра. ICANN несет ответственность за обеспечение безопасности и стабильности глобальной сети Интернет и выражает надежду на конструктивное сотрудничество с будущими операторами реестра gTLD для достижения этой цели.