Программа новых gTLD
Обновление справочного документа
Уменьшение последствий злонамеренных действий

Введение в программу новых gTLD

Компания ICANN основана десять лет назад как некоммерческая общественная организация с привлечением большого количества заинтересованных сторон. Целью ее создания явилось управление адресной системой Интернета. Одним из главенствующих принципов организации, признанным США и другими странами, стала поддержка конкурентной борьбы на рынке доменных имен, а также обеспечение безопасности и стабильности Интернета. Такое расширение общих доменов верхнего уровня (gTLD) позволит обновить и изменить систему адресов Интернета, в настоящее время представленную всего лишь 21 именем gTLD.

Решение о введении новой политики gTLDs было подготовлено длительными и глубокими обсуждениями, в которых принимали участие представители всех заинтересованных сторон глобального интернет-сообщества – правительственные и общественные организации, частные лица, коммерческие структуры, представители интеллектуальной и технической сфер. Существенный вклад в процесс разработки данной политики также внесли Государственный консультативный комитет ICANN (GAC), Расширенный консультативный комитет по делам индивидуальных пользователей (ALAC), Организация поддержки доменных имен индивидуальных стран (ccNSO) и Консультативный комитет по вопросам безопасности и стабильности (SSAC). В результате дискуссий была принята политика введения новых общих доменов верхнего уровня (gTLDs), которая была утверждена Организацией поддержки общих имен (GNSO) в 2007 году и одобрена Советом директоров ICANN в июне 2008 года. Начало программы запланировано на календарный 2010 год.

Данный справочный документ является одним из целой серии документов, опубликованных компанией ICANN для оказания помощи глобальному интернет-сообществу в вопросах, касающихся требований и процессов, представленных в проекте «Руководства кандидата».С конца 2008 года сотрудники компании ICANN представляют этапы процесса разработки программы на рассмотрение глобального интернет-сообщества, размещая в свободном доступе предварительные варианты руководства и другую сопроводительную документацию. Обсуждение ключевых материалов программы продолжается уже более 250 дней. Все комментарии подлежат тщательному анализу и используются при внесении коррективов в программу в процессе разработки финальной версии «Руководства кандидата».

Самые актуальные данные, сроки и мероприятия, связанные с Программой новых gTLD, см. по адресу

http://www.icann.org/en/tlds/select.htm

Обратите внимание, что это только предварительная версия документа, предназначенная для дальнейшего обсуждения. Потенциальные кандидаты не должны основываться исключительно на изложенных здесь положениях новой программы gTLD, поскольку программа все еще находится на рассмотрении и не утверждена.

Заключение

Разъяснительная работа, проведенная с общественностью по поводу уменьшения риска усиленного проявления злонамеренного поведения в связи с программой новых gTLD, дала значительные результаты.

Описанные в настоящем документе решения позволят значительно улучшить среду DNS, обеспечивая защиту для владельцев регистраций, более стабильную среду, а также инструменты для выявления потенциального злонамеренного поведения и борьбы с ним. Хотя эта область требует непрестанного усовершенствования, такие улучшения позволяют обеспечить стабильный запуск процесса новых gTLD. В условиях растущих требований к безопасности, обеспечение стабильности и отказоустойчивости всегда остается высокоприоритетной задачей для ICANN в процессе подготовки к запуску и реализации программы новых gTLD.

В этом направлении проделана большая работа, в основном, добровольцами из сообщества пользователей на форумах обсуждения и в рабочих группах. Именно они поспособствовали значительному улучшению среды DNS. Компания ICANN выражает им свою благодарность.

Этот документ является обновлением исходного справочного документа «Уменьшение последствий злонамеренных действий» («справочный документ о злонамеренном поведении»), опубликованного 3 октября 2009 года. Исходный справочный документ можно посмотреть по следующей ссылке:

http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

В исходном справочном документе о злонамеренном поведении компания ICANN обратилась к общественности с просьбой поделиться своими комментариями по поводу этого предложения, чтобы добавить конкретные меры в соглашение о регистрации новых gTLD, которые будут обязательными при всех регистрациях с целью уменьшения риска злонамеренного поведения в новых gTLD.

Чтобы упростить этот процесс, компания ICANN провела исследование злонамеренного поведения в рамках пространства TLD. В ходе этого исследования сотрудники ICANN прилагали усилия, чтобы получить комментарии из многочисленных внешних источников, включая Группу интеллектуальной собственности (IPC), Группу интернет-безопасности реестра (RISG), Консультативный комитет по безопасности и стабильности (SSAC), Группы реагирования на чрезвычайные компьютерные ситуации (CERT) и представителей банковской и финансовой сферы, а также сферы обеспечения интернет-безопасности. Эти стороны описали несколько проблем, связанных с потенциальным злонамеренным поведением, и порекомендовали компании ICANN найти способы их устранения или уменьшения их последствий в рамках соглашения о регистрации новых gTLD или в процессе подачи заявки. Эти рекомендованные меры направлены на укрепление общей безопасности и стабильности для владельцев регистраций и на рост доверия со стороны всех пользователей этих новых зон gTLD.

По результатам этого исследования и проведенного после него опроса общественности выработано девять общих рекомендаций, на основе которых можно создать элементы управления для уменьшения риска злонамеренного поведения в gTLD. Эти девять рекомендаций будут реализованы в программе:

1. ***Проверка операторов реестра.*** В соответствии с этой рекомендацией должна проводиться проверка операторов реестра для кандидатов на регистрацию новых gTLD, чтобы исключить совершение операторами преступных или злонамеренных действий в прошлом.
2. ***Демонстрация плана развертывания DNSSEC.*** В соответствии с этой рекомендацией кандидат на регистрацию нового gTLD обязательно должен предъявить план развертывания DNSSEC, что позволит уменьшить риск создания поддельных записей DNS.
3. ***Запрет подстановки.*** В соответствии с этой рекомендацией требуется внедрить элементы управления подстановкой DNS, чтобы уменьшить риск перенаправления DNS на вредоносные сайты.
4. ***Удаление потерянных записей.*** В соответствии с этой рекомендацией необходимо удалять записи DNS при удалении системы из gTLD, чтобы сократить риск использования таких оставшихся записей злоумышленниками.
5. ***Полные записи WHOIS.*** В соответствии с этой рекомендацией на gTLD необходимо вести «полные» записи WHOIS, чтобы обеспечить точность и полноту данных WHOIS. Использование полноформатных записей WHOIS обеспечивает ключевой механизм борьбы против злонамеренного использования новых gTLD, создавая более полную цепь контрактов в рамках TLD. Это, в свою очередь, должно ускорить поиск данных и решение проблем, связанных со злонамеренным поведением, по мере их обнаружения.
6. ***Централизация доступа к файлам зоны.*** В соответствии с этой рекомендацией учетные данные для доступа к данным файлов зоны реестра должны предоставляться через централизованный источник, чтобы обеспечить более точную и быструю идентификацию основных точек контакта внутри каждого TLD. Это позволяет сократить время, необходимое для выполнения корректирующих действий внутри TLD, в которых обнаружена злонамеренная деятельность.
7. ***Задокументированные контакты и процедуры в отношении злоупотребления на уровне реестра.*** В соответствии с этой рекомендацией gTLD должны установить единую точку контакта, которая отвечает за обработку жалоб на злоупотребление, а регистраторы должны предоставлять описание своей политики борьбы против злоупотребления. Эти требования рассматриваются как основные шаги для успешной борьбы со злонамеренным поведением в новых gTLD.
8. ***Участие в процессе ускоренных запросов безопасности реестра.*** В соответствии с этой рекомендацией новым gTLD предоставляется возможность быстро предпринимать эффективные действия в свете системных угроз для DNS путем создания выделенного процесса рассмотрения и утверждения ускоренных запросов безопасности.
9. ***Проект структуры для проверки зон высокой степени защиты.*** В соответствии с этой рекомендацией предлагается создать добровольную программу для выявления TLD, желающих установить и подтвердить повышенный уровень безопасности и надежности. Общая цель программы состоит в том, чтобы обеспечить механизм, позволяющий обозначить TLD как безопасные и надежные, для тех бизнес-моделей, которым будет выгоден такой знак отличия.

В остальных разделах справочного документа описывается состояние работы, проделанной в отношении каждой рекомендации.

Состояние реализации девяти рекомендаций в отношении злонамеренного поведения

В этом разделе описывается текущее состояние и/или обновления (если имеется) девяти рекомендаций, предложенных для уменьшения риска злонамеренного поведения в новых gTLD, в соответствии с исходным справочным документом о злонамеренном поведении (см. раздел «Сводка основных пунктов данного документа» выше). Каждая рекомендация разбита на два раздела: «Текущее состояние и/или обновления», где подробно описываются важные обновления в связи с рекомендацией, и «Конкретные рекомендуемые улучшения процесса новых gTLD», где в качестве ссылки предоставляется материал, опубликованный в справочном документе о злонамеренном поведении от 3 октября 2009 года.

1 Проверка операторов реестра

- **Текущее состояние и/или обновления**

  Эта рекомендация обязательно выполнять проверку истории операторов реестра является руководящим принципом в ходе усовершенствования процесса подачи заявки для кандидатов на регистрацию новых gTLD. Теперь процесс подачи заявки на регистрацию новых gTLD включает специальные критерии, в соответствии с которыми кандидат должен пройти различные биографические проверки в рамках оформления заявки. Кроме того, как говорится в исходном справочном документе о злонамеренном поведении, модуль 2 черновика Руководства кандидата содержит конкретные положения в отношении права отклонять кандидатов, если им не удастся пройти проверку, даже при выполнении ими остальных условий. Сведения о критериях и положениях модуля 2 черновика Руководства кандидата см. ниже или по ссылке:

  http://www.icann.org/en/topics/new-gtlds/draft-evaluation-criteria-30may09-en.pdf

2 Обязательное развертывание DNSSEC

- **Текущее состояние и/или обновления**

  Предъявление плана развертывания DNSSEC по-прежнему является обязательным компонентом процесса подачи заявки на регистрацию новых gTLD, а также частью тестирования перед делегированием для каждого нового gTLD. Документацию по данному требованию можно найти в модуле 5 черновика Руководства кандидата. Как в исходном справочном документе о злонамеренном поведении, спецификация 6 версии 3 соглашения о регистрации содержит положения относительно DNSSEC (см. ниже). Первое предложение в разделе 6 версии 3 изменено и теперь гласит: «Оператор реестра должен подписывать свои файлы зоны TLD, в которых реализованы расширения безопасности DNS («DNSSEC»)».

  ПРИМЕЧАНИЕ. RFC 4310 (как говорится ниже) обновлено до RFC 5910.

3 Запрет подстановки

- **Текущее состояние и/или обновления**

Положения, связанные с запретом подстановки DNS, остаются в составе спецификации 6 версии 3 соглашения о регистрации (см. раздел «Состояние в исходном справочном документе о злонамеренном поведении» ниже). Кроме того, 24 ноября 2009 года компания ICANN опубликовала справочный документ под названием «Опасность и угрозы со стороны замены NXDOMAIN (подстановка DNS и подобные технологии) на уровне реестра». В этом справочном документе описываются опасности и угрозы, связанные с заменой NXDOMAIN (которая чаще всего реализуется посредством подстановки DNS) на уровне реестра. В этом документе собраны выводы, опубликованные экспертами в данной области. Ссылка на исходный справочный документ:

http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm

В июне 2009 года на открытом заседании в Сиднее совет директоров ICANN постановил, что новые домены верхнего уровня не должны использовать переадресацию DNS и синтез ответов DNS.

В ответ на решение совета директоров, сотрудники ICANN включили запрет на переадресацию и синтез ответов DNS в черновик соглашения о регистрации новых gTLD. Компания ICANN также включила подобное обязательство в запрос на новые домены IDN ccTLD в документе «Общие положения и условия», а также в число предлагаемых вариантов отношений между ICANN и менеджером IDN ccTLD.

В заключение, совет директоров также поручил сотрудникам ICANN отчитываться об опасностях и угрозах, связанных с использованием переадресации и синтеза ответов DNS, то есть с подменой NXDOMAIN.

4 Поощрение удаления потерянных записей

- **Текущее состояние и/или обновления**

Комиссия SSAC сформировала рабочую группу для изучения этого вопроса. В настоящее время рабочая группа изучает файлы зон для всех текущих gTLD с целью учета потерянных серверов имен и, по возможности, определения того, в какой мере эти потерянные записи имен используются злоумышленниками. Рекомендации, предложенные рабочей группой SSAC, могут служить в качестве дополнительного руководства по управлению потерянными записями и будут рассматриваться на предмет включения в основные процессы gTLD.

Как говорится в исходном справочном документе о злонамеренном поведении, реестры должны предоставлять описание процесса удаления потерянных записей при удалении сервера имен из зоны (см. ниже).

5 Требование полных записей WHOIS

- **Текущее состояние и/или обновления**

Теперь вступила в силу рекомендация обязательного ведения «полных» записей WHOIS для всех новых gTLD. Все новые gTLD должны выполнять требования в отношении полных записей WHOIS в соответствии с последней версии соглашения о регистрации.

Кроме того, в черновик соглашения о регистрации в качестве комментария предварительно добавлена новая статья о том, что запись WHOIS должна быть доступной для поиска. Эта статья содержит следующее положение:

«Чтобы помочь предъявителям жалобы по UDRP определить, подпадают ли действия определенного владельца регистрации под определение "недобросовестность", информация WHOIS будет предоставляться в общедоступной базе данных в соответствии с действующей политикой конфиденциальности, а также будет доступна для поиска по имени домена, по имени владельца регистрации, по почтовому адресу владельца регистрации, по именам контактных лиц, по идентификаторам контактных лиц регистратора и по IP-адресу без каких-либо ограничений. С целью обеспечения производительности базы данных WHOIS может предоставляться поддержка логических операторов поиска».

Эта статья обеспечивает дополнительное средство для тех, кто занимается определением и предотвращением злонамеренного поведения в пространстве имен, при условии что методы и стандарты системы поиска имеют структуру управления, направленную на сокращение риска злонамеренного использования самой системы поиска. Эта статья имеется в некоторых существующих соглашениях о регистрации (.ASIA, .MOBI, .POST) и включена в данный черновик соглашения о регистрации новых gTLD для обсуждения. Например, система .NAME (http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm) на самом раннем этапе развертывания реализовала функцию поиска по «расширенным записям WHOIS». Функция поиска основана на многоуровневой модели доступа, которая позволяет уменьшить риск ее злонамеренного использования. Мы ждем комментариев в отношении того, как именно это требование может способствовать предотвращению определенных типов злонамеренного поведения, а также альтернативных предложений по эффективному использованию данных WHOIS для зарегистрированных имен в контексте уменьшения проявления злонамеренного поведения в новых gTLD. Если это требование будет поддержано, мы также ждем предложения по разработке единой технической спецификации для функции поиска.

6 Централизация доступа к файлам зоны

- **Текущее состояние и/или обновления**

Компания ICANN приняла рекомендацию по созданию механизма для поддержки централизованного доступа к записям файла зоны, в результате этого была создана консультативная группа под названием «Консультативная группа по доступу к файлам зоны» («Консультативная группа ДФЗ»). Эта группа должна в сотрудничестве с общественностью создать проект механизма для поддержки централизованного доступа к файлам зоны. Консультативная группа ДФЗ завершила работу по стратегическому предложению, которое можно просмотреть по ссылке:

http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf

Следующим шагом на пути централизации доступа к файлам зоны является реализация рекомендаций, описанных в предложении.

7 Задокументированные контакты и процедуры в отношении злоупотребления на уровне реестра

- **Текущее состояние и/или обновления**

В соответствии с этой рекомендацией, все новые gTLD должны документировать контакты и процедуры в отношении злоупотреблений конкретного реестра и описывать свои конкретные политики против злоупотребления. Это положение не изменялось с момента публикации исходного справочного документа о злонамеренном поведении (см. ниже).

8 Участие в процессе ускоренных запросов безопасности реестра

- **Текущее состояние и/или обновления**

В соответствии с кратким изложением в исходном справочном документе о злонамеренном поведении, компания ICANN опубликовала справочный документ под названием «Процесс ускоренных запросов безопасности реестра» (см. ниже). В нем дается определение процесса «Ускоренный запрос безопасности реестра» (УЗБР). Этот процесс стал результатом сотрудничества компании ICANN и регистраторов gTLD по разработке процесса быстрого реагирования в случаях, когда регистраторы gTLD:

- сообщают ICANN о возникшем или угрожающем инциденте безопасности в отношении их TLD и/или DNS и
- запрашивают договорной отказ для действий, которые они предприняли или могут предпринять с целью уменьшения последствий или устранения инцидента.

Контрактный отказ представляет собой освобождение от необходимости соблюдать определенное положение соглашения о регистрации на период времени, необходимый для устранения или уменьшения последствий инцидента.

Теперь доступна веб-процедура отправки запроса УЗБР, с ней можно ознакомиться в приложении A или по следующей ссылке:

http://www.icann.org/en/registries/ersr/.

Этот новый процесс должен использоваться регистраторами gTLD только для тех инцидентов, которые требуют от них немедленных действий с целью предотвращения пагубного воздействия на стабильность или безопасность DNS. Для обеспечения стабильности DNS этот процесс был сразу введен в силу с 1го октября 2009 года. Дополнительные сведения о запросе УЗБР можно получить по ссылке:

http://www.icann.org/en/announcements/announcement-01oct09-en.htm

9 Проект структуры для проверки зон высокой степени защиты

- **Текущее состояние и/или обновления**

Заинтересованные группы в области финансов и банковского (такие как BITS) дела порекомендовали создать проект структуры для проверки зон высокой степени защиты, и создана инициатива под названием «Программа доменов верхнего уровня высокой степени защиты» («Программа ДВУВС3 (HSTLD)»). Целью этой инициативы является создание проекта структуры предложенных элементов управления для проверки зон высокой степени защиты. С целью анализа возможных подходов к созданию такой структуры и подготовки предложения для вынесения на суд общественности компания ICANN учредила консультативную группу по доменам верхнего уровня высокой степени безопасности («Консультативная группа ДВУВС3»). Эта группа уполномочена в сотрудничестве с общественностью, используя модель восходящей разработки, подготовить и предложить подход(ы) к добровольной программе, которая включает стандарты управления и поощрения с целью укрепления безопасности и надежности TLD, которые принимают решение участвовать в этой программе.

В настоящее время консультативная группа ДВУВС3 состоит из членов сообщества, которые проявили желание посодействовать программе, а также из экспертов в областях, связанных с программой (таких как безопасность, аудит, программы сертификации, финансовые службы), и сотрудников ICANN. Консультативная группа ДВУВС3 регулярно проводит совещания с целью обсуждения концепций, выдвинутых в исходном документе от октября 2009 года, проектирования элементов управления и формулировки требований программы, а также планирует публикацию практической программы действий с целью ознакомления общественности и получения отзывов. Консультативная группа ДВУВС3 ведет работу и готовит программу в ходе открытого и прозрачного процесса. Дополнительные сведения, включая список участников группы и протоколы еженедельных заседаний консультативной группы ДВУВС3, можно найти по ссылке:

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

Компания ICANN не будет заниматься реализацией программы. Независимый орган установит критерии, в соответствии с которыми будет проводить сертификацию TLD. Этот орган будет отвечать за мониторинг и продление сертификатов, а также за их публикацию.

Приложение A

Процесс ускоренных запросов безопасности реестра

Ускоренный запрос безопасности реестра (УЗБР – ERSR) разработан с целью предоставления регистраторам gTLD процедуры, которая позволяет им информировать компанию ICANN о возникшем или угрожающем инциденте (далее «Инцидент») безопасности в отношении их TLD и/или DNS, чтобы запросить контрактный отказ для действий, которые они предприняли или могут предпринять с целью уменьшения последствий или устранения инцидента. Контрактный отказ представляет собой освобождение от необходимости соблюдать определенное положение соглашения о регистрации на период времени, необходимый для устранения или уменьшения последствий инцидента. Запрос УЗБР создан для того, чтобы обеспечить операционную безопасность в случае Инцидента и соответствующее уведомление затрагиваемых сторон (например, ICANN, других затрагиваемых поставщиков).

Инцидент может относиться к одной или нескольким из следующих категорий:

- злонамеренное действие, затрагивающее DNS, масштаб и критичность которого подвергают угрозе безопасность, стабильность и отказоустойчивость системы TLD или DNS;
- несанкционированное раскрытие, изменение, добавление или уничтожение данных регистрации или несанкционированный доступ к информации или ресурсам в Интернете системами, функционирующими в соответствии со всеми применимыми стандартами;
- случайность, которая может привести к кратковременному или долговременному отказу одной или нескольких критически важных функций регистратора gTLD в соответствии с определением в опубликованном ICANN Плане по обеспечению непрерывности работы реестра gTLD [PDF, 96 КБ].

Запрос УЗБР применяется исключительно для Инцидентов, то есть для событий, требующих немедленных действий со стороны регистратора и быстрого ответа в течение трех (3) рабочих дней со стороны ICANN. Этот процесс не заменяет запросы, которые следует оформлять в соответствии со Стратегией оценки услуг реестра (RSEP).

Мы признаем, что в некоторых экстраординарных случаях регистраторам требуется предпринимать немедленные действия с целью предотвращения или устранения Инцидента. При возникновении подобных Инцидентов регистраторы должны как можно скорее отправить запрос УЗБР, чтобы при необходимости компания ICANN могла предоставить отказ с обратной силой.

Регистраторы могут отправлять запросы УЗБР путем заполнения формы на странице http://www.icann.org/cgi/registry-sec. Отправленный запрос обрабатывается следующим образом:

- Запрос УЗБР автоматически отправляется в группу реагирования по вопросам безопасности ICANN, а отправителю посылается копия запроса. Группа реагирования по вопросам безопасности состоит из сотрудников следующих департаментов: отдел безопасности, отдел связей с регистраторами gTLD, юридический отдел и отдел соответствия.
- Назначенный участник группы реагирования по вопросам безопасности, занимающийся конкретным запросом, обязан связаться с регистратором в течение одного (1) рабочего дня для подтверждения инцидента и получения дополнительной информации, если это необходимо.
- Группа реагирования по вопросам безопасности может при необходимости запросить дополнительную информацию, которая требуется для оценки и рассмотрения запроса УЗБР. В таком случае отправителю запроса рекомендуется оперативно предоставить такую информацию.
- Группа реагирования по вопросам безопасности собирается в течение двух (2) рабочих дней с момента получения запроса (и запрошенной дополнительной информации) с целью его рассмотрения и принятия решения.
- Компания ICANN дает устный и письменный ответ отправителю или назначенному им представителю в течение трех (3) рабочих дней после получения запроса УЗБР.
- Назначенный участник группы реагирования по вопросам безопасности поддерживает связь с основным контактным лицом регистратора на протяжении всего периода устранения Инцидента.
- Если запрос получен после того, как регистратор устранил Инцидент, компания ICANN попытается ответить в течение десяти (10) рабочих дней в письменной форме, чтобы в ответ на запрос предоставить отказ с обратной силой, если это необходимо.
- После ответа на запрос УЗБР группа реагирования по вопросам безопасности в сотрудничестве с регистратором составляет отчет о результатах работы, который можно опубликовать для общественности. Если требуется опубликовать отчет о результатах работы, компания ICANN и регистратор согласовывают, какие разделы запроса УЗБР и отчета необходимо изменить с целью обеспечения конфиденциальности и защиты проприетарной информации. Компания ICANN и регистратор могут убирать из публикации информацию, которую они обоснованно считают конфиденциальной или проприетарной.