Программа введения новых доменов gTLD
Объяснительный меморандум

Предотвращение злонамеренного поведения

Дата публикации: 3 октября 2009 г.

Общая информация: программа введения новых доменов gTLD

Поскольку ICANN была основана 10 лет назад как некоммерческая многосторонняя организация для координации системы адресации в Интернете, одним из ее принципов, признанных США и другими государствами, является стимулирование конкуренции на рынке доменных имен с одновременным обеспечением безопасности и стабильности Интернета. Расширение общих доменов верхнего уровня (gTLD) увеличит возможности использования инноваций, выбора и изменений в системе адресации в Интернете, которая сейчас представлена 21 доменами gTLD.

Решение ввести новые домены gTLD стало результатом долгих и подробных консультаций со всеми структурами глобального интернет-сообщества, представленными самыми различными участниками — правительственными структурами, отдельными лицами, гражданскими организациями, сообществами бизнеса и организациями по защите интеллектуальной собственности, а также технологическим сообществом. Свой вклад внесли также следующие подразделения ICANN: Правительственный консультационный комитет (Governmental Advisory Committee, GAC), Расширенный консультативный комитет (At-Large Advisory Committee, ALAC), Организация по поддержке национальных доменов (Country Code Names Supporting Organization, ccNSO) и Комитет по вопросам безопасности и стабильности (Security and Stability Advisory Committee, SSAC). Процесс консультаций привел к выработке политики введения новых доменов gTLD, сформулированной Организацией поддержки родовых имен (Generic Names Supporting Organization (GNSO) в 2007 г. и принятой Правлением ICANN в июне 2008 г. Начало реализации программы запланировано на 2010 календарный год.

Настоящий объяснительный меморандум входит в набор документов, опубликованных организацией ICANN для доведения до сведения глобального интернет-сообщества требований и процессов, изложенных в Руководстве заявителя (Applicant Guidebook) (на данный момент в виде предварительной версии). С конца 2008 г. сотрудники ICANN информируют интернет-сообщество о ходе процесса разработки программы через ряд открытых форумов, посвященных предварительным версиям руководства заявителя и связанных документов. На данный момент было организовано более 250 дней консультаций, посвященных важнейшим областям программы. Полученные замечания внимательно анализируются и используются для дальнейшего уточнения условий программы и для разработки окончательной версии Руководства заявителя.

Текущая информация и информация о временных рамках и мероприятиях, относящихся к программе введения новых доменов gTLD, представлена на веб-сайте http://www.icann.org/en/topics/new-gtld-program.htm.

Обратите внимание, что это только предварительная версия для обсуждения. Потенциальные

заявители не должны руководствоваться изложенными здесь положениями программы введения новых доменов gTLD, поскольку программа является предметом обсуждения и доработки.

Резюме основных пунктов данного документа

Организация ICANN заинтересована в получении замечаний относительно предложения добавить конкретные меры в соглашении о реестре новых доменов gTLD (описаны ниже), которые будут обязательны для всех реестров в целях предотвращения потенциальных случаев злонамеренного поведения.

В процессе исследования злонамеренного поведения сотрудники ICANN запросили и получили информацию из нескольких внешних источников, среди которых Рабочая группа по борьбе с фишингом (Anti-Phishing Working Group, APWG), Группа реестров по безопасности в Интернете (Registry Internet Safety Group, RISG), Комитет по вопросам безопасности и стабильности (Security and Stability Advisory Committee, SSAC), Компьютерные группы экстренного реагирования (Computer Emergency Response Teams, CERTs) и члены банковского/финансового сообщества и сообщества безопасности в Интернете. Эти источники описали несколько потенциальных проблем, относящихся к злонамеренному поведению, и поддержали ICANN в поиске средств устранения этих проблем или смягчения их последствий в соглашениях о новых реестрах доменов gTLD. Эти рекомендованные меры призваны увеличить преимущества общей безопасности и стабильности для регистрантов и доверие всех пользователей к этим новым зонам gTLD.

В отзывах, полученных на версию 2 предварительного варианта Руководства заявителя (Draft Applicant Guidebook) во время собрания в Сиднее и во время консультаций после Сиднея, содержатся рекомендации относительно мер и средств контроля для предотвращения злонамеренного поведения, которые должны быть включены в виде требований в предварительную версию базового соглашения о реестре для новых доменов gTLD. Ниже приведены основные пункты полученных отзывов и процесс, использованный при подготовке этих рекомендаций.

Рекомендации содержат конкретные меры по снижению риска злонамеренного поведения в девяти областях:

1. Проверенные операторы реестров
2. Продемонстрированный план развертывания DNSSEC
3. Запрещение использования подстановочных знаков
4. Удаление изолированных связующих (glue) записей при удалении записи сервера имен из зоны
5. Требование "толстых" записей Whois
6. Централизованный доступ к файлам зон
7. Задокументированные контакты и процедуры на уровне реестра для сообщений о незаконном использовании
8. Участие в процессе ускоренного запроса безопасности реестра (Expedited Registry Security Request, ERSR)

9. Предварительная базовая структура для проверки зон высокой безопасности (High Security Zones Verification)

Мы считаем, что в комплексе эти меры позволят существенно снизить риск появления злонамеренного поведения в новых доменах gTLD. Разработка политики для этих проблем и выработка мер, принимаемых для снижения риска злонамеренного поведения, будут продолжены. ICANN может также рассмотреть возможность формирования рабочей группы, состоящей из представителей систем обеспечения безопасности и членов сообщества ICANN, для оказания помощи в разработке и оценке решений и конкретных реализаций предлагаемых мер защиты.

Введение

Поскольку ICANN была основана 10 лет назад как некоммерческая многосторонняя организация для координации системы адресации в Интернете, одним из ее основополагающих принципов, признанных многими правительствами и другими участниками, является стимулирование конкуренции на рынке доменных имен с одновременным обеспечением безопасности и стабильности Интернета. Расширение вызовет инновацию, новые возможности выбора и позитивные изменения в системе адресации в Интернете. В мире, насчитывающем 1,5 миллиарда пользователей Интернета, многообразие, широкий выбор и конкуренция являются ключевыми факторами успеха и распространения всемирной сети.

Решение открыть эти раунды приема заявок по новым доменам gTLD стало итогом долгих и подробных дискуссий, в которых принимали участие все организации глобального интернет-сообщества. Представители различных участников (правительств, частных лиц, гражданского общества, бизнес-сообщества, организаций по защите интеллектуальной собственности, технологического сообщества) участвовали в обсуждениях в течение более 18 месяцев. В октябре 2007 г. Организация поддержки родовых имен (Generic Names Supporting Organization, GNSO), одна из групп ICANN по координации глобальной политики Интернета, завершила работу по разработке политики в отношении новых доменов gTLD и утвердила набор рекомендаций. Кульминацией этого процесса разработки политики стало решение о принятии разработанной сообществом политики, принятое Советом директоров ICANN на совещании ICANN в июне 2008 г. в Париже. Подробное изложение процесса политики и результатов представлено на веб-сайте http://gnso.icann.org/issues/new-gtlds/.

Настоящий документ входит в набор документов, которые публикуются организацией ICANN в качестве объяснительных меморандумов, которые призваны помочь интернет-сообществу лучше понять запрос о представлении предложений Request for Proposal (RFP), также называемый "Руководство заявителя" (Applicant Guidebook). Период сбора публичных комментариев для Руководства заявителя (Applicant Guidebook) и этих документов сформирует базу, на основе которой будет осуществлен подробный пересмотр и исправление этих идей. Эти комментарии будут использованы для редактирования документов в процессе подготовки окончательной версии Руководства заявителя (Applicant Guidebook).

Обратите внимание, что это только предварительная версия для обсуждения. Потенциальные заявители не должны руководствоваться изложенными здесь положениями программы введения новых доменов gTLD, поскольку программа является предметом обсуждения и доработки.

Отклики сообщества относительно проблемы злонамеренного поведения

Организация ICANN получила многочисленные публичные комментарии, относящиеся к различным областям, в ответ на анонсированное расширение пространства доменов TLD путем делегирования новых доменов TLD (включая домены TLD с доменными именами IDN). Одна из проблем, которая была указана несколькими участниками, касалась потенциально возросших возможностей

злонамеренного поведения, связанных с новыми доменами gTLD. Чтобы найти решение этой проблемы, организация ICANN запросила комментарии у экспертов (относительно реагирования на злонамеренное поведение) и у участников, пострадавших от злонамеренного поведения в существующих доменах gTLD.

Отклики, полученные на более ранние версии 1 и 2 предварительного варианта Руководства заявителя (Draft Applicant Guidebook), служат важным первичным источником при разработке рекомендаций, которые будут включены в версию 3 предварительного варианта Руководства заявителя (Draft Applicant Guidebook).

Вторым источником информации относительно этой проблемы является корпус выпущенных комитетом SSAC отчетов о формах злонамеренного поведения. В частности, это относится к отчетам SAC038 "Registrar Abuse Point of Contact" (Точка контакта регистратора для сообщения о незаконном использовании) (pdf) и SAC040 "Measures to Protect Domain Registration Services Against Exploitation or Misuse" (Меры защиты служб регистрации доменов от эксплуатации или неправомерного использования) (pdf). Эти отчеты и другие материалы, составленные комитетом SSAC, содержат рекомендации и инструкции относительно лучших решений для реестров и регистраторов, на основе которых были предложены изменения предварительного варианта Руководства заявителя (Draft Applicant Guidebook) и соглашения о реестре новых доменов gTLD.

Третьим источником является предварительная версия отчета, подготовленная Рабочей группой по борьбе с фишингом (APWG) — отраслевой ассоциацией, занимающейся предотвращением краж идентификационных сведений и мошенничества, которые являются результатом возросшей проблемы фишинга и спуфинга электронной почты. Этот отчет был согласован с Комитетом по политике в Интернете (Internet Policy Committee, IPC) APWG, который включает более 90 членов, представляющих самые разные категории участников APWG. Следует отметить, что многие участники ICANN (в том числе реестры и регистраторы доменов gTLD и ccTLD, поставщики услуг Интернета, владельцы интеллектуальной собственности, организации по обеспечению безопасности и финансовые учреждения) являются членами APWG и комитета IPC APWG, см. http://www.antiphishing.org/sponsors.html. Комитет IPC APWG считает, что запланированное расширение доменов gTLD станет важным событием, которое потенциально может оказать воздействие на возможности электронной преступности. Отчет IPC APWG содержит полную и конструктивную информацию для ICANN относительно многих вопросов, касающихся злонамеренного поведения, которые, по мнению IPC APWG, заслуживают внимания и планирования во время развертывания новых доменов gTLD.

Четвертый источник информации был предоставлен Группой реестров по безопасности в Интернете (RISG) — глобальной группой ответственных организаций, относящихся к Интернету, совместно работающих над борьбой с хищением идентификационных данных через Интернет, в особенности с фишингом и распространением вредоносных программ. В отчете RISG (pdf) перечислены несколько проблем, которые могут возникнуть из-за увеличения числа реестров.

Пятым источником исходной информации, касающейся проблемы злонамеренного поведения, является ряд комментариев, полученных от представителей банковского и финансового сообщества. Своим опытом в этой

области поделились такие отраслевые ассоциации, как BITS Fraud Reduction Program, American Banking Association, Financial Services Information Sharing and Analysis Center (*FS-ISAC*) и Financial Services Technology Consortium (FSTC). Благодаря уникальным знаниям и опыту в области обеспечения безопасности как сетей, так и конфиденциальных данных, это сообщество предоставило ценные конкретные рекомендации относительно мер (в частности, внедрение безопасных бизнес-практик), которые реестры должны реализовать для повышения доверия пользователей и снижения риска ущерба от вредоносных атак.

Шестым источником исходной информации, касающейся мер по предотвращению злонамеренного поведения в новых доменах gTLD, являются материалы работы, сделанной группой IRT (Implementation Recommendation Team). Хотя организация ICANN определила защиту товарных знаков и потенциальную опасность злонамеренного использования как отдельные важнейшие проблемы, которые необходимо решить при образовании новых доменов gTLD, имеется существенное сходство подходов, предлагаемых для устранения этих проблем. Резюме работы группы IRT представлено в "Открытом письме группы IRT с описанием нашей работы" (Open Letter from the IRT Introducing our Work) от 29 мая 2009 г. Группа IRT была сформирована Комитетом по интеллектуальной собственности (Intellectual Property Constituency) ICANN в соответствии с решением Правления ICANN от 6 марта 2009 г. (ссылка) по просьбе представителей сообщества, занимающихся поиском решения по предотвращению потенциальных рисков держателей товарных знаков при внедрении новых доменов gTLD. Отчет, предоставленный группой IRT (pdf), отражает разнообразный опыт и национальную специфичность 18 членов группы и их 2-х помощников.

Другие источники исходной информации были предоставлены сообществом служб экстренной помощи по безопасности в Интернете. Ценные советы предоставили члены таких организаций, как международный Форум служб безопасности и реагирования на инциденты (Forum of Incident Response and Security Teams, FIRST), в который входят группы по экстренному реагированию на проблемы с компьютерным и сетевым оборудованием из 180 корпораций, правительственных организаций, университетов и других учреждений, которые расположены в Серверной и Южной Америке, Азии, Европе и Океании и помогают вести борьбу с киберпреступностью. Члены различных правоохранительных органов предоставили помощь в определении важных проблем и предложили изменения в операциях реестров, которые помогут в борьбе с интернет-преступностью.

Кроме указанных источников информации, организация ICANN использовала информацию, полученную от участников публичных консультаций, проведенных в Сиднее, Нью-Йорке, Лондоне, Гонконге и Абу-Даби. В рамках этих консультаций проводились отдельные заседания, посвященные проблеме сокращения возможностей злонамеренного поведения в новых доменах gTLD.

ICANN поддерживает на веб-сайте icann.org вики-среду, посвященную сбору информации о потенциальных решениях проблемы злонамеренного поведения в новых доменах gTLD. Упомянутые выше отчеты были опубликованы в этой вики-среде с приглашением к участию в обсуждении и отправке комментариев.

Выявленные основные проблемы

В процессе обсуждения в ICANN эти различные участники выявили ряд проблем, относящихся к возможностям злонамеренного поведения. Хотя многие из этих проблем относятся к уникальным и сложным техническим уязвимостям и требуют различных средств контроля и учета различных обстоятельств, их можно обобщить и классифицировать по следующим основным тематическим категориям:

A. Как гарантировать, что недобросовестные лица не будут управлять реестрами?

Источники рекомендовали ICANN принять меры для снижения риска того, что увеличившееся число реестров приведет к проникновению в сообщество ненадежных операторов или преступников, которые будут способствовать злонамеренному поведению.

B. Как обеспечить целостность и полезность информации реестра?

Источники рекомендуют ICANN воспользоваться созданием новых доменов gTLD для повышения качества регистрации доменных имен и служб разрешения доменных имен так, чтобы ограничить возможности злонамеренного поведения.

C. Как обеспечить более эффективную борьбу с уже выявленными случаями незаконного использования?

Принимая во внимание, что злонамеренное поведение уже существует и затрагивает все домены TLD, источники призывали ICANN при установлении новых доменов TLD использовать имеющиеся процессы и средства для снижения имеющегося уровня киберпреступности и незаконного использования в системе DNS и системах регистрации доменов.

D. Как обеспечить усиленную инфраструктуру контроля для доменов TLD с имеющимися потенциальными возможностями незаконного использования?

Некоторые новые домены TLD могут предполагать совершение транзакций по электронной почте, для которых требуется высоконадежная инфраструктура (например, электронные финансовые службы или голосование через Интернет), и могут затрагивать критически важные активы и инфраструктуру (например, обеспечивающие инфраструктуру энергетики или медицинских учреждений), которым необходимо обеспечить повышенную защиту от лиц, уже занимающихся злонамеренным поведением через систему доменных имен. Источники рекомендовали, чтобы ICANN предприняла меры по созданию системы, обеспечивающей повышенное доверие для операций в таких зонах.

Предлагаемые меры по миграции:

Чтобы устранить описанные выше проблемы злонамеренного поведения, ICANN считает необходимым принять ряд мер в рамках планирования внедрения новых доменов gTLD. Помимо повышенных обязательств со стороны реестров новых доменов gTLD в их контрактах с ICANN, этим новым реестрам рекомендуется оговорить более жесткие стандарты ведения бизнеса и меры по обеспечению безопасности с аккредитованными регистраторами. В частности, реестр нового

домена gTLD будет иметь возможность требовать, чтобы регистраторы внедрили конкретные меры по снижению риска злонамеренного поведения для регистрации имен в своей зоне.

Кроме того, ICANN продолжит совместно с сообществом дополнять выработку существующей политики и усилия рабочей группы по выработке защитных мер, которые должны будут внедряться в интерфейсе регистратор-регистрант.

Ниже приведены общие категории предлагаемых защитных мер, которые должны быть включены в текущую версию предварительного варианта Руководства заявителя (Draft Applicant Guidebook):

1. Проверенные операторы реестров
2. Продемонстрированный план развертывания DNSSEC
3. Запрещение использования подстановочных знаков
4. Удаление изолированных связующих (glue) записей при удалении записи сервера имен из зоны
5. Требование "толстых" записей Whois
6. Централизованный доступ к файлам зон
7. Задокументированные контакты и процедуры на уровне реестра для сообщений о незаконном использовании
8. Участие в процессе ускоренного запроса безопасности реестра (Expedited Registry Security Request, ERSR)
9. Предварительная базовая структура для проверки зон высокой безопасности (High Security Zones Verification)

Проблемы и соответствующие защитные меры

A. Как гарантировать, что недобросовестные лица не будут управлять реестрами?

1. Проверенные операторы реестров

B. Как обеспечить целостность и полезность информации реестра?

2. Требование развертывания DNSSEC
3. Запрет использования подстановочных символов
4. Рекомендация удаления изолированных связующих (glue) записей

C. Как обеспечить более целенаправленную борьбу с уже выявленными примерами незаконного использования?

5. Требование "толстых" записей Whois
6. Централизованный доступ к файлам зон
7. Задокументированные контракты и политики борьбы с незаконным использованием на уровне реестра и регистраторов
8. Доступность процесса ускоренного запроса безопасности реестра

(Expedited Registry Security Request, ERSR)

D. Как обеспечить усиленную инфраструктуру контроля для доменов TLD с имеющимися потенциальными возможностями злонамеренного поведения?

9. Программа проверки зон высокой безопасности

Конкретные меры, которые должны быть реализованы в контрактах новых реестров

Следующие меры включены в Руководство заявителя (Applicant Guidebook) и отражают процедуры, требуемые для всех новых реестров. Место формулировки в предварительном варианте Руководства заявителя (Draft Applicant Guidebook) определено. Приведена также краткая аргументация для каждой конкретной меры (выделена курсивом).

1. Проверенные операторы реестров

Вопрос заявителя (приложение к Модулю 2) гласит:

ICANN может отклонить по следующим причинам заявку, удовлетворяющую всем прочим условиям:

Заявитель или любой сотрудник, партнер, директор или менеджер или другое связанное лицо, или любое физическое или юридическое лицо, владеющее (или владеющее на праве собственности) 15% или более компании-заявителя:

а) в течение последних 10 лет был признан виновным в уголовном преступлении или правонарушении, связанным с неправомерным управлением финансами или компанией, или был судим судом за совершение мошенничества или нарушения попечительской обязанности, или в отношении него было выдано судебное определение, которое ICANN считает существенным эквивалентом любого из перечисленных выше пунктов;

б) в течение последних 10 лет был наказан государственным или отраслевым надзорным органом за поведение, предполагающее нечестность или неправомочное использование чужих средств;

в) в данный момент вовлечен в судебный процесс или регулятивное производство, которое может завершиться приговором, решением, определением или наказанием одного из типов, перечисленных в пункте (а) или (б);

г) является объектом дисквалификации, наложенной организацией ICANN, которая действует на момент рассмотрения заявки; или

д) на момент подачи заявки не предоставил организации ICANN идентификационную информацию, необходимую для подтверждения идентификации

е) является объектом ряда решений, указывающих на ответственность за недобросовестность (или повторные случаи такой недобросовестности) в отношении регистрации доменных имен, в том числе:

(i) приобретение доменных имен преимущественно в целях продажи, аренды или иного вида передачи регистраций доменных имен владельцу товарного знака или знака обслуживания или конкуренту для извлечения выгоды, превышающей задокументированные прямые расходы, относящиеся к доменному имени; или

(ii) регистрирование доменных имен в целях предотвращения того, чтобы владелец товарного знака или знака обслуживания мог отразить свой знак в соответствующем доменном имени; или

(iii) регистрирование доменных имен преимущественно в целях нарушения бизнеса конкурента; или

(iv) использование доменных имен с намерением привлечь пользователей Интернета с коммерческой выгодой на веб-сайт или другое местоположение в Интернете путем введения в заблуждение за счет сходства с товарным знаком или знаком обслуживания в отношении источника, спонсора, связи или поддержки веб-сайта, местоположения, продукта или услуги на веб-сайте или местоположении.

Примечание. Информация, собранная в ходе этих перекрестных проверок (включая сведения о прошлой преступной деятельности) будет рассматриваться в процессе обработки заявки.

Процесс обработки заявки будет включать стандартизированные тщательные перекрестные и контрольные проверки компаний и физических лиц (например, основных сотрудников). Эта мера позволит снизить риск того, что признанные преступниками лица, члены преступных организаций или лица, имеющие случаи неправомерного ведения бизнеса, будут участвовать в операциях реестра или получат контроль (напрямую или через подставных лиц) над реестрами.

2. Требование развертывания DNSSEC

Операторы реестров будут обязаны предоставить задокументированный план для подписи файла зоны и иметь реализованную технологию DNSSEC на момент начала операций.

Следующая формулировка была добавлена в спецификацию 6 версии 3 Соглашения реестра (подлежит технической редакции):

"Оператор реестра должен внедрить технологию DNSSEC (Domain Name System Security Extensions). В течение периода действия Оператор реестра должен соответствовать требованиям документов RFC 4033, 4034, 4035, 4509 и 4310 и заменяющих их документов и следовать лучшим решениям, описанным в документе RFC 4641 и заменяющих его документах. Если Оператор реестра внедряет технологию Hashed Authenticated Denial of Existence для DNS Security Extensions, она должна соответствовать документу RFC 5155 и заменяющих его документам. Оператор реестра должен принимать материал открытого ключа от дочерних доменных имен безопасным образом в соответствии с отраслевыми лучшими решениями. Реестр также должен опубликовать на своем веб-сайте документ о практиках и политике (также называемый "DNSSEC Policy Statement" или "DPS"), в котором описывается хранение материала ключей, доступ и

использование для собственных ключей и материала "точки доверия" регистрантов."

Преимущества для общей безопасности и стабильности Интернета, получаемые за счет внедрения технологии DNSSEC, хорошо задокументированы. ICANN обязуется подписать корневую зону в течение 2009 года и обеспечит возможность использования этого важного средства повышения безопасности DNS при установлении новых доменов gTLD.

3. Запрет использования подстановочных символов

В отчете SAC041 комитета SSAC (одобрен Правлением ICANN) и отчетах других организаций, предоставивших комментарии, организации ICANN рекомендуется запретить новым доменам TLD использовать перенаправление DNS и синтезированные ответы DNS.

С учетом текущей тенденции использования вредоносного ПО, связанного с сайтами с рекламными материалами, перенаправление доменов на рекламные сайты представляет потенциально повышенный риск злонамеренного поведения. Для доменных имен, не зарегистрированных регистрантом, или для которых регистрант не предоставил действительных записей (таких как записей о серверах имен (NS)) для записи в файле зоны DNS, или статус которых не позволяют им быть опубликованными в DNS, запрещается использование DNS-записей ресурсов с подстановочными знаками (как описано в RFC 4592) или любой другой метод или технология синтезирования DNS-записей ресурсов, или использование реестром перенаправления в DNS. В частности, в случае запроса таких доменных имен заслуживающие доверия серверы имен должны возвращать ответ "Ошибка имени" (также называемый NXDOMAIN), RCODE 3, как описано в RFC 1035 и связанных с ним документах RFC.

Это положение применяется для всех файлов зон DNS на всех уровнях дерева DNS, для которого оператор реестра (или филиал, участвующий в предоставлении услуг регистрации) поддерживает данные, организует такую поддержку или извлекает доход из такой поддержки.

Следующее запрещение использования подстановочных знаков было добавлено в спецификацию 6 версии 3 Соглашения реестра:

"Для доменных имен, не зарегистрированных регистрантом, или для которых регистрант не предоставил действительных записей (таких как записей о серверах имен (NS)) для записи в файле зоны DNS, или статус которых не позволяют им быть опубликованными в DNS, запрещается использование DNS-записей ресурсов с подстановочными знаками (как описано в RFC 4592) или любой другой метод или технология синтезирования DNS-записей ресурсов, или использование реестром перенаправления в DNS. В случае запроса таких доменных имен заслуживающие доверия серверы имен должны возвращать ответ "Ошибка имени" (также называемый NXDOMAIN), RCODE 3, как описано в RFC 1035 и связанных с ним документах RFC. Это положение применяется для всех файлов зон DNS на всех уровнях дерева DNS, для которого оператор реестра (или филиал, участвующий в предоставлении услуг регистрации) поддерживает данные, организует такую поддержку или извлекает доход из такой поддержки.

В отчете SAC041 (pdf) комитета SSAC и отчетах других организаций, предоставивших

комментарии, организации ICANN рекомендуется запретить новым доменам TLD использовать перенаправление DNS и синтезированные ответы DNS. Опасности, связанные с перенаправлением и синтезированными ответами, не только в доменах TLD, но также на подчиненных уровнях DNS. Это положение в новых контрактах реестров имеет целью устранить эту проблему на уровне реестра.

4. Рекомендация удаления изолированных связующих (glue) записей

В своих опубликованных политиках борьбы с незаконным использованием реестры должны предоставить описание способа удаления изолированных связующих (glue) записей при удалении записи сервера имен из зоны. Ниже приведена выдержка из вопросов заявителей в предварительном варианте Руководства заявителя (Draft Applicant Guidebook) (модуль 2):

"Предотвращение незаконного использования и смягчение его последствий. Заявители должны описать предлагаемые политики и процедуры для сведения к минимуму незаконных регистраций и других действий, имеющих негативные последствия для пользователей Интернета… Ответы должны включать систему быстрого освобождения или приостановки и *предлагаемые меры по отслеживанию и удалению изолированных связующих (glue) записей для имен, удаленных из зоны.*"

Согласно исследованию APWG, примерно 3% доменов, использованных для фишинга, использовали записи "изолированных серверов имен", т.е. остатки домена, ранее удаленного из реестра. Это создает потенциальное "безопасное убежище" в виде записи сервера имен в файле зоны того домена TLD, который злоумышленники могут использовать для поддержки злонамеренных регистраций доменов.

5. Требование "толстых" записей Whois

Оператор реестра должен поддерживать и предоставлять открытый доступ к данным регистрации с помощью модели "толстых" данных Whois, как это требуется в спецификации 4 версии 3 формы соглашения реестра.

"Служба WHOIS. До тех пор пока ICANN не укажет другой формат и протокол, оператор реестра будет управлять службой публикации данных регистрации как через порт 43, так и через веб-сайт <whois.nic.(TLD)> в соответствии с требованиями RFC 3912, предоставляя открытый доступ на основе запросов к следующему минимальному набору элементов в следующем формате. ICANN сохраняет за собой право указать другие форматы и протоколы, включая IRIS (Internet Registry Information Service) (RFC 3981 и связанные с ним документы RFC), и после появления такой спецификации оператор реестра реализует такую альтернативную спецификацию в течение разумно необходимого периода времени."

Организация ICANN предложила изменить требования для службы Whois в предлагаемом новом соглашении реестра таким образом, чтобы все реестры были обязаны предлагать "толстые" записи Whois, как описано в предыдущем объяснительном меморандуме (pdf). Кроме того, в предварительной версии отчета (pdf) Группы по рекомендациям для внедрения (Implementation Recommendations Team, IRT), сформированной Комитетом по интеллектуальной собственности (Intellectual Property Constituency) ICANN, говорится, что "IRT считает, что требование предоставления информации службы WHOIS на уровне реестра в соответствии с

моделью "толстой" WHOIS исключительно важно для экономичной защиты потребителей и владельцев интеллектуальной собственности." Реализация "толстой" модели WHOIS поможет снизить риск злонамеренного поведения за счет обеспечения более высокой доступности и улучшенной стабильности доступа к записям.

6. Централизованный доступ к файлам зон

ICANN будет требовать, чтобы реестры разрешали доступ к данным файлов зон для обеспечения их доступности через централизованного поставщика.

Предложенная версия спецификации 4 соглашения реестра (подлежит технической редакции) гласит, что оператор реестра сделает эти данные доступными для сообщества в целом:

"2.2.1. Общий доступ. Оператор реестра должен предоставить постоянный общий доступ к файлам зон для домена TLD организации ICANN или назначенному ей лицу таким способом, который может время от времени определяться организацией ICANN.

"2.2.2. Центральное хранилище файлов зон. В случае если организация ICANN или назначенное ей лицо определит центральное хранилище файлов зон, оператор реестра предоставляет все данные файлов зон организации ICANN или по просьбе ICANN стороннему оператору такого хранилища, назначенного организацией ICANN. Если такое центральное хранилище файлов определено, ICANN может отказаться, исключительно на усмотрение ICANN, от соответствия требованиям раздела 2.1 данной спецификации 4. [Этот раздел 2.2.2 включен для обсуждения сообществом в результате предыдущих обсуждений сообществом проблем предотвращения злонамеренного поведения. Согласно этому положению, назначенное организацией ICANN лицо может взять на себя ответственность (в данный момент возложенную на операторов реестров) по проверке и мониторингу доступа к данным файлов зон, осуществляемого ответственными лицами для законных целей.]"

Чтобы облегчить доступ к данным файлов зон, который в данный момент осуществляется отдельными реестрами, организация ICANN (или организация, назначенная организацией ICANN для выполнения этой функции) собирает данные файлов зон у реестров новых доменов gTLD и предоставляет подписчикам электронный доступ к этим данным. Это также предполагает наличие единого контракта, который должны подписать стороны, желающие получить доступ к файлам зон реестров, регулируемых ICANN. ICANN составляет контракты на доступ на основе текущей модели и обеспечивает администрирование/поддержку системы передачи.

Такая централизованная координация позволит сообществу по борьбе с незаконным использованием эффективно получать обновления о новых доменах по мере их создания в каждой зоне.

7. Задокументированные контракты и политики для борьбы с незаконным использованием на уровне реестра и регистраторов

Оператор реестра должен обеспечить наличие единой точки контакта для

сообщения о незаконном использовании для всех доменов в пределах домена TLD. Эта точка контакта для сообщения о незаконном использовании используется для устранения проблем и своевременного реагирования на жалобы о незаконном использовании, полученных от уполномоченных сторон (например, других реестров, регистраторов, правоохранительных органов и уполномоченных членов сообщества по борьбе с незаконным использованием). Реестры также обязаны предоставить описание своих политик по борьбе с незаконным использованием.

Оператор реестра может потребовать от всех регистраторов, с которыми он заключает контракты на обслуживание, чтобы они обеспечили наличие точки контакта для сообщения о незаконном использовании. Эта мера соответствует рекомендациям, приведенным в отчете комитета SSAC SAC038 (pdf). Реестры могут также потребовать, чтобы регистраторы опубликовали задокументированную политику борьбы с незаконным использованием, соответствующую политике борьбе с незаконным использованием, принятой в реестре. На обоих уровнях политика должна содержать процедуры для выполнения следующих действий:

1. приостанавливать действие доменов, определенных как участвующие в незаконном использовании товарных знаков, фишинге, целенаправленном распространении вредоносных программ или другой незаконной или мошеннической деятельности;
2. устранять проблемы реселлеров и других контролируемых ими дистрибьюторов;
3. удалять изолированные связующие (glue) записи;
4. определять точку контакта для сообщения о незаконном использовании и способ связи с этой точкой контакта.

Для решения этой проблемы в спецификацию 6 версии 3 Соглашения реестра была добавлена следующая формулировка:

"Оператор реестра должен предоставить на своем веб-сайте точные контактные данные, в том числе действительный адрес электронной почты и почтовый адрес, а также координаты основного контактного лица, отвечающего за обработку запросов, относящихся к злонамеренному поведению в домене TLD, и предоставлять организации ICANN своевременные уведомления о любых изменениях этих контактных данных."

Кроме того, следующий фрагмент вопроса модуля 2 включен в предварительный вариант Руководства заявителя (Draft Applicant Guidebook), версия 3:

"… Каждый оператор реестра обязан установить и опубликовать на своем веб-сайте единую точку контакта для сообщения о незаконном использовании, отвечающую за разрешение вопросов, требующих быстрого реагирования и обеспечивающую своевременный отклик на жалобы о незаконном использовании, относящиеся ко всем именам, зарегистрированных в домене TLD всеми записанными регистраторами, в том числе подразумевающими участие реселлера."

Реализация (возможно, широкомасштабная) новых реестров требует введения новых четко определенных средств контроля и установленных ролей в процессе

регистрации домена. Реализация контактов и политик для борьбы с незаконным использованием на уровне реестра и регистраторов будет важнейшим шагом, который позволит продолжать и расширять усилия по борьбе со злонамеренным поведением по мере добавления новых операторов.

8. Доступность процесса ускоренного запроса безопасности реестра (Expedited Registry Security Request, ERSR)

На основе опыта, полученного при реагировании на появление червя Conficker, организация ICANN в сотрудничестве с реестрами доменов gTLD, регистраторами и экспертами по безопасности разработала дополнительную процедуру (http://www.icann.org/en/announcements/announcement-01oct09-en.htm) для создания процесса, с помощью которого реестры смогут информировать ICANN о наличии (или возможности появления) ситуации угрозы безопасности, затрагивающей домен gTLD, и запросить отказ от контрактных обязательств для действий, которые реестр может предпринять или предпринял для уменьшения или устранения проблем безопасности.

Ситуация угрозы безопасности определяется как сочетание одного или нескольких из следующих факторов:

a. злонамеренные действия, затрагивающие DNS и имеющие такой масштаб и серьезность, что они угрожают систематической безопасности, стабильности и отказоустойчивости DNS;

b. потенциальное или фактическое неавторизованное раскрытие, изменение, дополнение или уничтожение данных реестра или неавторизованный доступ к информации или ресурсам (или их раскрытие) в Интернете с помощью систем, работающих согласно всем применимым стандартам;

c. потенциальные или фактические нежелательные последствия, которые могут вызвать временный или долгосрочный сбой (или угрозу такого сбоя) одной или нескольких критически важных функций реестра gTLD, как это определено в Плане обеспечения непрерывности реестров доменов gTLD (gTLD Registry Continuity Plan) ICANN (pdf).

Процесс запроса ERSR предназначен исключительно для инцидентов, которые требуют немедленного действия со стороны реестра и экстренного отклика (в течение 24–48 часов) со стороны ICANN. Этот процесс не предполагает замещения запросов, которые должны делаться согласно политике оценки услуг реестра (Registry Services Evaluation Policy, RSEP) (ссылка).

9. Программа проверки зон высокой безопасности

Чтобы удовлетворить нужду сообщества в повышенном доверии для отдельных доменов gTLD, организация ICANN создала предварительную базовую структуру для программы проверки доменов gTLD. В текущей предлагаемой версии эта программа будет исключительно добровольной.

Решение не участвовать в проверке на момент подачи заявки на новый домен gTLD НЕ ОТРАЖАЕТСЯ негативно на заявителе и никак не отражается на его баллах, полученных в процессе оценки. Целью программы проверки является создание приемлемого набора стандартов и критериев для повышения доверия для

проверенных доменов gTLD за счет применения соответствующих средств контроля операций и безопасности и измерение производительности работы реестров и регистраторов доменов gTLD относительно этих средств контроля. Реестры доменов gTLD, прошедшие проверку, смогут открыто отображать статус прохождения проверки каким-либо образом — например, путем отображения "знака" (или маркировки), право отображения которого можно будет проверить по главному списку прошедших проверку доменов gTLD. ICANN будет вести и публиковать главный список прошедших проверку доменов gTLD.

Кроме ведения главного списка прошедших проверку доменов gTLD, роль ICANN в реализации программы заключается в помощи в выработке, уточнении и координации управления программой и в совместной с сообществом работой над стандартами и критериями программы. Фактическая оценка соответствия доменов gTLD стандартам и критериям программы будет выполняться независимыми организациями.

Для прохождения проверки в рамах предлагаемой программы операции реестра должны соответствовать следующим принципам (см. Руководство, модуль 2):

a. Реестр демонстрирует, что оператор поддерживает эффективные средства контроля для обеспечения гарантии того, что безопасность, доступность и конфиденциальность систем и информационных активов, обеспечивающих выполнение критически важных ИТ-операций и бизнес-операций реестра поддерживается на должном уровне.

b. Реестр поддерживает эффективные средства контроля для обеспечения гарантии того, что выполнение основных функций реестра авторизовано и осуществляется точно, полностью и в срок в соответствии с установленными политиками и стандартами. Участвующие стороны идентифицируются, и для них выполняется аутентификация.

c. Реестр поддерживает эффективные средства контроля для обеспечения разумной гарантии того, что выполнение основных функций регистратора его регистраторами авторизовано и осуществляется точно, полностью и в срок в соответствии с установленными политиками и стандартами. Участвующие стороны идентифицируются, и для них выполняется аутентификация.

В число процессов, необходимых для успешного прохождения проверки, входят проверка операций реестра и поддержка операций регистратора.

Если заявитель выбирает прохождение проверки, это осуществляется в два этапа.

Этап I

Перед делегированием нового домена gTLD заявитель участвует в проведении оценки, которая включает в себя следующие элементы:

- Фоновая информация
- Процедуры, относящиеся к управлению доменом/освобождению оборудования
- Точка контакта для сообщения о незаконном использовании и реагирование

- Процедуры резервирования записей

После того как новый домен gTLD делегирован и начал функционировать, заявителю будет предоставлен определенный период времени на реализацию всех предварительно утвержденных процессов и средств контроля.

Этап II

В ходе следующего этапа тестируются процессы, средства контроля и процедуры, задокументированные в ходе Этапа 1, и проверяется их правильное функционирование. Если обнаруживаются недостатки, независимый орган, проводящий проверку, сообщает о них организации ICANN . Оператору реестра предоставляется определенное время для устранения проблемы перед тем, как на запрос заявителя о прохождении проверки будет дан отрицательный ответ. В этом последнем случае оператор реестра должен подать повторную заявку на прохождение проверки позднее.

Если проверка заявки реестра нового домена gTLD завершается и домен TLD делегирован, в этот момент оператор реестра может принять решение о прохождении проверки; в этом случае он проходит описанные выше тесты в один этап. Другими словами, заявитель может по своему желанию выполнить действия для прохождения проверки после завершения процесса оценки (когда его новый домен gTLD уже функционирует), а не одновременно с процессом оценки.

Средства контроля, обязательные для прохождения проверки, оцениваются периодически путем прохождения аудитов для сохранения статуса прошедшего проверку домена gTLD.

ICANN считает, что такая программа проверки обеспечивает повышенный уровень доверия в сертифицированных доменах gTLD за счет расширения требований для обеспечения точности средств контроля обработки для реестра, регистраторов и регистрантов, а также для операций реестра и регистраторов. Баланс между доверием и преимуществами/затратами составляет главный бизнес-фактор, на основе которого реестр домена gTLD будет принимать решение о целесообразности использования проверки как бизнес-процесса.

Программа проверки применяется к предлагаемому набору действий, необходимых для поддержания высокого доверия к операциям реестра. Основное внимание в предварительной базовой структуре сосредоточено на средствах контроля, необходимых для уменьшения возможностей злонамеренного поведения в реестрах доменов gTLD, которые примут решение о получении знака проверки от ICANN. Сфера действия ограничена средствами контроля и действиями на уровне операций реестра и регистраторов и не распространяется на операции регистрантов. Программа проверки призвана обеспечить разумно достаточную, но не абсолютную гарантию того, что проверенные домены gTLD имеют эффективно функционирующие средства контроля, удовлетворяющие критериям проверки. Поэтому определение критериев проверки и периодические независимые проверки/аудиты их эффективности в рамках программы проверки обеспечат повышенный уровень доверия.