



Механизмы защиты Программы New gTLD от злоупотребления DNS

Исследование деятельности и политики ICANN | Март 2016 года

Содержание

ВВЕДЕНИЕ	1
ЗЛОУПОТРЕБЛЕНИЕ DNS: КЛЮЧЕВАЯ ТЕРМИНОЛОГИЯ	4
РАБОЧАЯ ГРУППА ПО ПОЛИТИКЕ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ЗЛОУПОТРЕБЛЕНИЯМИ РЕГИСТРАЦИИ	7
ЗЛОУПОТРЕБЛЕНИЕ DNS: КЛЮЧЕВАЯ СТАТИСТИКА И ТЕНДЕНЦИИ	13
Злоупотребления DNS в новых gTLD	15
АНАЛИЗ ПРИМЕРОВ ЗЛОУПОТРЕБЛЕНИЯ DNS: ФИШИНГ В НОВЫХ gTLD	17
ДЕВЯТЬ МЕХАНИЗМОВ ЗАЩИТЫ	19
ВОПРОС: КАК МЫ ОБЕЗОПАСИМ СЕБЯ ОТ УПРАВЛЕНИЯ РЕГИСТРАТУРАМИ НЕДОБРОСОВЕСТНЫМИ СУБЪЕКТАМИ?	20
МЕХАНИЗМ ЗАЩИТЫ: ПРОВЕРКА ОПЕРАТОРОВ РЕГИСТРАТУРЫ	21
ВОПРОС: КАК МЫ ОБЕСПЕЧИМ ЦЕЛОСТНОСТЬ И ПОЛЕЗНОСТЬ ИНФОРМАЦИИ О РЕГИСТРАТУРЕ?	23
МЕХАНИЗМ ЗАЩИТЫ: ТРЕБОВАТЬ ДЕМОНСТРАЦИЮ ПЛАНА ПО РАЗВЕРТЫВАНИЮ DNSSEC	23
МЕХАНИЗМ ЗАЩИТЫ: ЗАПРЕТ НА ИСПОЛЬЗОВАНИЕ СИМВОЛОВ ОБОБЩЕНИЯ ИМЕНИ	25
МЕХАНИЗМ ЗАЩИТЫ: УДАЛЕНИЕ ПОТЕРЯННЫХ СВЯЗУЮЩИХ ЗАПИСЕЙ	28
ВОПРОС: КАК МЫ ОБЕСПЕЧИМ БОЛЕЕ ЦЕЛЕНАПРАВЛЕННУЮ РАБОТУ ПО БОРЬБЕ С ИДЕНТИФИЦИРОВАННЫМ ЗЛОУПОТРЕБЛЕНИЕМ?	30
МЕХАНИЗМ ЗАЩИТЫ: ТРЕБОВАНИЕ ЗАПИСЕЙ ЦЕНТРАЛИЗОВАННОГО WHOIS	30
МЕХАНИЗМ ЗАЩИТЫ: ЦЕНТРАЛИЗАЦИЯ ДОСТУПА К ФАЙЛАМ ЗОН	32
МЕХАНИЗМ ЗАЩИТЫ: ДОКУМЕНТАЛЬНОЕ ОФОРМЛЕНИЕ КОНТАКТОВ И ПРОЦЕДУР ПО ВОПРОСАМ ЗЛОУПОТРЕБЛЕНИЙ НА УРОВНЕ РЕГИСТРАТУР	34
МЕХАНИЗМ ЗАЩИТЫ: УЧАСТИЕ В ПРОЦЕДУРЕ ЗАПРОСА НА СРОЧНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РЕГИСТРАТУРЫ (ERSR)	35
ВОПРОС: КАК МЫ ОБЕСПЕЧИМ УЛУЧШЕННУЮ КОНЦЕПЦИЮ УПРАВЛЕНИЯ ДЛЯ TLD С ВНУТРЕННИМ ПОТЕНЦИАЛОМ ЗЛОУПОТРЕБЛЕНИЯ?	36
МЕХАНИЗМ ЗАЩИТЫ: СОЗДАТЬ ПРОЕКТ КОНЦЕПЦИИ ДЛЯ ПРОГРАММЫ ПРОВЕРКИ ЗОН С ВЫСОКОЙ СТЕПЕНЬЮ БЕЗОПАСНОСТИ	36
ПРЕДЛОЖЕНИЕ И МОДЕЛИ ИССЛЕДОВАНИЯ	38
ВОЗМОЖНАЯ КАЧЕСТВЕННАЯ КОНЦЕПЦИЯ ДЛЯ ТЕСТИРОВАНИЯ ЭФФЕКТИВНОСТИ МЕХАНИЗМОВ ЗАЩИТЫ	40
План проведения исследования: Ключевые вопросы и соображения	40
КАУЗАЛЬНЫЕ МОДЕЛИ И ГИПОТЕЗЫ	42
ПРИЛОЖЕНИЕ: ИССЛЕДОВАНИЕ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ СО ЗЛОУПОТРЕБЛЕНИЕМ В ICANN	45

Введение

В соответствии с разделом 9.3 документа [«Подтверждение обязательств»](#) (AoC) ICANN, в целях роста конкуренции, потребительского доверия и потребительского выбора в системе доменных имен (DNS), данный отчет предназначен для оказания содействия работе группы по анализу конкуренции, потребительского доверия и потребительского выбора (CCT-RT). Это будет достигнуто посредством:

- Предоставления общего обзора состояния злоупотребления DNS в результате развертывания Программы новых доменов общего пользования (верхнего уровня) (gTLD) в январе 2012 года
- Обсуждения вариантов средств измерения эффективности девяти механизмов защиты, внедренных для сведения к минимуму злоупотреблений в новых gTLD
- Предложения исследовательской модели, способной оценить эффективность девяти механизмов защиты, внедренных для сведения к минимуму злоупотреблений в новых gTLD

Согласно [AoC](#):

ICANN проведет проверку, охватывающую то, насколько расширение gTLD способствовало росту конкуренции, потребительского доверия и потребительского выбора, а также эффективность **...механизмов защиты, внедренных для сведения к минимуму проблем, связанных с ...расширением...** [выделено автором]. Проверка будет осуществляться на добровольной основе участниками сообщества, а состав соответствующей группы по анализу будет опубликован для общественного обсуждения... Полученные по результатам проверки рекомендации будут переданы Правлению и опубликованы для общественного обсуждения. Правление обязуется принять меры в течение шести месяцев после получения рекомендаций

Для подготовки к потенциальному расширению DNS, ICANN обратилась за консультацией к экспертной группе интересов, чтобы та исследовала потенциальную возможность роста неправомерной, злонамеренной и преступной деятельности в расширенной DNS и предоставила рекомендации по **превентивному сведению к минимуму** такой деятельности посредством набора **механизмов защиты**.¹ Попытка идентифицировать шаги по сведению к минимуму потенциальной возможности злоупотреблений началась с четырех вопросов, заданных экспертам из неоднородного набора групп, включая Антифишинговую

¹ “Mitigating Malicious Conduct,” ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

рабочую группу (APWG), Группу по безопасности интернет-регистратуры (RISG), Консультативный комитет по безопасности и стабильности (SSAC), Компьютерную группу реагирования на чрезвычайные ситуации (CERT) и членов банковских, финансовых сообществ и сообщества по безопасности в интернете. Эти вопросы звучали так:

- 1) Как мы обезопасим себя от управления регистратурами недобросовестными субъектами?
- 2) Как мы обеспечим целостность и полезность информации о регистратуре?
- 3) Как мы обеспечим более целенаправленную работу по борьбе с идентифицированным злоупотреблением?
- 4) Как мы обеспечим улучшенную концепцию управления для TLD с внутренним потенциалом злонамеренного поведения?

По результатам обширных консультаций, экспертные группы пришли к указанным ниже **рекомендациям** для устранения проблем в области каждого вопроса:

Вопрос	Рекомендация(-ии)
1) Как мы обезопасим себя от управления регистратурами недобросовестными субъектами?	1) Проверить операторов регистратуры посредством проведения проверки анкетных данных в целях снижения риска того, что потенциальный оператор регистратуры был причастен к преступному, злонамеренному и/или недобросовестному поведению.
2) Как мы обеспечим целостность и полезность информации о регистратуре?	2) Требовать развертывания расширения безопасности системы доменных имен (DNSSEC) со стороны всех новых регистратур, чтобы минимизировать вероятность подставных записей DNS. 3) Запретить «использование символов обобщения имени» во избежание переадресации DNS и синтезированных ответов DNS, которые могут привести к попаданию на вредоносные сайты. 4) Стимулировать удаление потерянных связующих записей , чтобы свести к минимуму использование этих следов доменов, ранее удаленных из записей о

	<p>регистратуре, в качестве безопасных записей сервера имен в файле корневой зоны TLD, который могут использовать злонамеренные субъекты.</p>
<p>3) Как мы обеспечим более целенаправленную работу по борьбе с идентифицированным злоупотреблением?</p>	<p>5) Требовать записи централизованного WHOIS, чтобы стимулировать доступность и полноту данных WHOIS.</p> <p>6) Централизовать доступ к файлу корневой зоны для создания более эффективных способов получения обновлений по новым доменам по мере их создания внутри каждой зоны TLD.</p> <p>7) Документально зафиксировать контакты и политику по вопросам злоупотреблений на уровне регистратур и регистраторов, чтобы обеспечить единый контактный орган по работе с жалобами на злоупотребление.</p> <p>8) Обеспечить процедуру запроса на срочное обеспечение безопасности регистратуры для работы с угрозами безопасности, которые требуют немедленного принятия мер от регистратуры и срочного ответа от ICANN.</p>
<p>4) Как мы обеспечим улучшенную концепцию управления для TLD с внутренним потенциалом злонамеренного поведения?</p>	<p>9) Создать проект концепции для программы проверки зон с высокой степенью безопасности, чтобы установить набор критериев, обеспечивающих надежность TLD, которые с большей вероятностью могут стать целью злонамеренных субъектов — например, банковские или фармацевтические TLD — посредством улучшения оперативного контроля и управления безопасностью.</p>

Основная цель работы CCT-RT заключается в измерении эффективности этих механизмов защиты. В целях оказания содействия этой работе, данный отчет представит тщательное исследование каждого из этих механизмов защиты, предложит потенциальные способы измерения их эффективности (по возможности) и представит исследовательскую модель для точного и всестороннего анализа их эффективности. Обратите внимание, что данный отчет предназначен для *содействия* CCT-RT. Он предназначен для того, чтобы предложить *возможные* методы и побудить группу к обсуждению того, как лучше всего обойтись с их исследованием злоупотребления DNS и механизмов защиты, внедренных для сведения его к минимуму, в контексте Программы New gTLD.

Злоупотребление DNS: Ключевая терминология

«Злоупотребление DNS» охватывает широкий спектр деятельности. Несмотря на отсутствие принятого на мировом уровне определения, варианты определений могут включать в себя «киберпреступность», «хакерство» и, как в прошлом использовала ICANN, «злонамеренное поведение». Исследователи Римского университета и Глобального центра информационной безопасности классифицируют подобные угрозы DNS как попадающие под три категории: повреждение данных, отказ в обслуживании и частная жизнь.²

«Злоупотребление DNS» – это термин, используемый в данном отчете, относящийся к намеренно обманной, потворствующей или нежелательной деятельности, в которой активно используется DNS и/или процедуры, используемые для регистрации доменных имен. Это рабочее определение, основывающееся на анализе того, какая деятельность, как правило, анализируется в литературе как злонамеренная или неправомерная, и направлено на то, чтобы дать CCT-RT отправную точку для усовершенствования собственного определения злоупотребления DNS в их работе. Как раскрывается далее, некоторые виды деятельности попадают в категорию «недобросовестных» — но необязательно незаконных — способов ведения коммерческой деятельности, в то время как другие представляют собой откровенные махинации, которые, вероятно, являются незаконными в большинстве юрисдикций по всему миру. Вопрос о том, насколько каждый вид злоупотребления (описанный ниже) попадает под это определение и может быть проанализирован с точки зрения девяти механизмов защиты для сведения к минимуму злоупотребления DNS в Программе New gTLD, останется открытым для рассмотрения CCT-RT. Цель состоит в предоставлении рабочей структуры определения, которая

² Casalicchio, Caselli, and Coletta, “Measuring the Global Domain Name System,” IEEE Network 27, no. 1, (2013) 25-31. doi: 10.1109/MNET.2013.6423188

бы вписалась в дополнительное обсуждение вопроса о том, какие виды деятельности необходимо включить в их работу.

Злоупотребление DNS: Тактики и инструменты

Как правило, злонамеренные субъекты реализуют свои схемы следующими способами:³

- **Взломанные домены:** домены, в которых злонамеренный субъект взломал веб-хостинг владельца домена.
- **Злонамеренные регистрации:** домены, зарегистрированные злонамеренными субъектами для непосредственной цели, заключающейся в злоупотреблении DNS.
- **Перекупщики субдоменов:** услуги — многие из которых бесплатны и предлагают анонимную регистрацию за пределами сервиса WHOIS — которые позволяют людям создавать регистрации на третьем уровне под доменом второго уровня, которым владеет поставщик услуг. У таких перекупщиков часто нет никакой регистрации или контактной информации кроме имен учетной записи пользователя.⁴
- **IP адреса:** иногда в URL фишинговых атаках используются IP-адреса, а не доменные имена.
- **Сокращенные URL:** метод сжатия длинных доменных адресов, который может быть использован злонамеренными субъектами, чтобы запутать доменное имя и таким образом переадресовать ничего не подозревающих пользователей на вредоносные сайты.⁵

Несмотря на то, что злоупотребление DNS может принимать множество форм, как правило, оно направлено на распространение **вредоносного ПО** – расшифровывается как «вредоносное программное обеспечение» – которое используется для нарушения компьютерных операций, сбора конфиденциальной информации или получения доступа к системам личного

³ Обратите внимание, что злонамеренные субъекты, в основном, используют первые два способа. См. Illumintel, “Potential for Phishing in Sensitive-String Top-Level Domains,” study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

⁴ Anti-Phishing Working Group, “Making Waves in the Phisher’s Safest Harbor: Exposing the Dark Side of Subdomain Registries,” November 2008, http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

⁵ См. StopTheHacker.com, “The Curse of the URL Shorteners: How Safe Are They?” по состоянию на 26 февраля 2016 года, <https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/>

компьютера.⁶ Само по себе вредоносное ПО может осуществлять разнообразную вредную деятельность и принимать различные формы. Самые часто распространяемые программы включают:

- **Вирусы:** Вредоносные программы могут осуществлять разнообразную нежелательную деятельность и вызывать ненадлежащую работу компьютера, включая создание, перемещение и/или удаление файлов и/или потребление памяти компьютера. Часто они себя воспроизводят и путешествуют по сетям посредством зараженных электронных писем. Примеры включают «червей» и «троянских коней».⁷
- **Шпионское ПО:** Вредоносное ПО может собирать данные, например, имена пользователей, пароли, информацию о кредитных картах, тенденции просмотра веб-страниц и электронные письма.⁸

Вредоносное ПО часто распространяется через использование **ботов**, которые представляют собой автоматизированные программы, запрограммированные на постоянную работу для выполнения вредоносных или неправомерных функций.⁹ **Бот-сети** – это сети таких ботов, которые используют зараженные компьютеры для распространения вредоносного ПО.¹⁰ Владельцы атакованных компьютеров не знают, что их устройства используются в подобных целях.

⁶ “Implementation Advisory Group for Competition, Consumer Choice, and Consumer Trust (IAG-CCT): Final Recommendations on Metrics for CCT Review,” 26 September 2014, <https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf>

⁷ Kaspersky Lab, “What is a Computer Virus or a Computer Worm?” по состоянию на 26 февраля 2016 года, <http://www.kaspersky.com/internet-security-center/threats/viruses-worms>

⁸ Kaspersky Lab, “What is Spyware?” по состоянию на 26 февраля 2016 года, <http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY>

⁹ Часто боты не являются вредоносными и выполняют ряд легальных функций. Однако в данном отчете говорится только об их вредоносной форме. См. Gabada, Usman, and Sharma, “Techniques to Break the Botnet Attack,” International Journal for Research in Emerging Science and Technology 2, no. 1 (March 2015), <http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf>

¹⁰ Из того же источника.

Рабочая группа по политике в сфере противодействия злоупотреблениями регистрацией

В 2010 году Рабочая группа по политике в сфере противодействия злоупотреблениями регистрацией (RAPWG) GNSO предоставила отчет, в котором исследовались положения о злоупотреблении в соглашениях между регистратурой и регистратором. В этом отчете группа пришла к единому определению злоупотребления – а именно:

Злоупотребление – это действие, которое а) причиняет фактический или существенный вред, или является обоснованным основанием вреда, и б) является незаконным или неправомерным, или по иным основаниям считается противоречащим заявленным намерениям и планам законного использования, если цель использования была раскрыта.¹¹

Они пошли дальше и разграничили злоупотребление «**регистрацией**» и «**использованием**», где первое означает проблемы, возникающие во время регистрации доменов, а второе – то, как домены используются после регистрации. Их концепция определения выглядит следующим образом:

Проблемы при регистрации связаны с основной деятельностью регистраторов и регистратур, относящейся к доменным именам. В общем случае к этой деятельности относится (помимо прочего) распределение зарегистрированных имен; сопровождение регистрационной информации (WHOIS) и обеспечение доступа к ней; передача, удаление и перераспределение доменных имен; а также аналогичные области, которые в дальнейшем обсуждаются более подробно. Все вышеперечисленное в целом охвачено процессом разработки политики GNSO. Многие из этих видов деятельности специально перечислены в соглашениях о регистрации как деятельность, подлежащая включению в согласованные политики, а существующие согласованные политики должны охватывать перечисленные темы.

Группа обсуждала следующие виды деятельности как потенциальные формы злоупотреблений регистрацией:

- **Киберсквоттинг** – преднамеренная и недобросовестная регистрация и использование имени, которое является зарегистрированной маркой или торговым знаком, несвязанным с организацией, часто в целях получения прибыли (как правило, но не ограничиваясь, посредством рекламных объявлений с платой за щелчок).
- **Опережение** – когда какая-либо сторона получает некое подобие инсайдерской информации, касающейся предпочтений интернет-

¹¹ “Registration Abuse Policies Working Group Final Report,” May 2010, <http://gns0.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf>

пользователя в отношении регистрации доменного имени и использует эту возможность для заблаговременной регистрации этого доменного имени.

- **Сайты для критики** – интернет-сайты, которые жалуются на продукты или услуги компании или организации и используют товарный знак компании в доменном имени (например, `companysucks.example`). Группа выразила обеспокоенность тем, что эти типы сайтов потенциально способны нарушить права владельцев товарного знака. Однако группа также отметила, что во многих случаях подобные сайты являются площадкой для обоснованных жалоб и защищены законами о свободе слова во многих юрисдикциях.
- **Вводящие в заблуждение и/или оскорбительные доменные имена** – регистрация доменных имен, которая направляет ничего не подозревающих потребителей к нежелательному контенту или направляет несовершеннолетних к вредному содержанию — иногда называется видом «мышеловки».
- **Поддельные уведомления о продлении** – заведомо ложная корреспонденция, отправленная владельцам домена от индивидуального лица или организации, которая заявляет себя или представляет действующего регистратора. Они отправляются в совершенно разнообразных целях для введения в заблуждение.
- **Вращение имени** – использование автоматизированных инструментов для создания перестановок данной строки доменного имени. Несмотря на то, что регистраторы регулярно используют подобные инструменты на законном основании, чтобы предложить альтернативные строки потенциальным владельцам доменов, если строка, запрашиваемая владельцем домена, недоступна, группу обеспокоил тот факт, что подобные инструменты могли привести к нарушению строк, содержащих товарный знак.
- **Плата за щелчок** – модель размещения рекламы в интернете, используемая на интернет-сайтах, на которых рекламодатель оплачивает хост только при нажатии на его рекламу. Был поднят вопрос об использовании товарного знака в доменном имени для привлечения посетителей на сайт, содержащий оплаченную рекламу о размещении.
- **Отвлечение трафика** – использование торговых названий в видимом тексте HTML, скрытом тексте, мета-тегах или заголовке интернет-страницы для управления рейтингом поисковых служб и отвлечения трафика.
- **Ложное образование филиала** – обманное заявление себя филиалом владельца торгового названия.
- **Махинация с перекрестной регистрацией TLD** – обманная торговая практика, при которой существующему владельцу домена отправляется уведомление о том, что другая сторона заинтересована или пытается зарегистрировать доменную строку

владельца домена в другом TLD. Таким образом, владельца домена вынуждают пройти дополнительные регистрации с помощью стороны, которая отправила уведомление – часто ею является перекупщик, который получает прибыль от дополнительных регистраций и предлагает новый домен по цене выше среднерыночной.

- **«Дегустация»/«охота на домены»** – когда владельцы домена злоупотребляют льготным периодом пробного использования доменного имени путем постоянной регистрации, удаления и повторной регистрации одних и тех же имен, чтобы избежать оплаты регистрационных сборов.

В отличие от этого, RAPWG определила проблемы «использования» как:

Проблемы использования доменных имен относятся к действиям владельца регистрации со своим доменным именем после создания домена — назначением домена, выбранным для него владельцем регистрации, и/или услугами, которые владелец регистрации предоставляет с помощью этого домена. Эти проблемы использования часто не зависят от или не включают в себя проблемы регистрации... использование доменных имен – это область, в которой полномочия ICANN и GNSO при разработке политики более ограничены.

Группа обсуждала следующие виды деятельности как потенциальные формы злоупотреблений использованием:

- **Фишинг** – интернет-сайт, обманным образом представляющий себя в качестве надежного сайта (часто банка), чтобы выманить у интернет-пользователей конфиденциальную информацию (например, учетные данные интернет-банкинга, пароли от электронной почты. Как правило, цель фишинга состоит в краже средств или других ценных активов.
- **Спам** – целый ряд нежелательных электронных писем, отправляемых доменом и используемых для рекламы интернет-сайтов.
- **Управление и контроль вредоносного ПО/бот-сетей** – использование доменных имен как способ управления и обновления бот-сетей, которые представляют собой сети, содержащие от нескольких тысяч до нескольких миллионов зараженных компьютеров, находящиеся под общим управлением преступника. Бот-сети могут использоваться для осуществления многих видов злонамеренной деятельности, включая **атаки типа «отказ в обслуживании» (DDOS)**, **спам** и фишинг хостингов с технологией **Fast Flux** и спам-сайты (более подробное объяснение случаев применения и терминологии, использованной в этом определении, см. ниже).

- **Использование украденных учетных данных** – например, учетных данных личности, доступа или финансов для регистрации доменных имен в злонамеренных целях, кражи и/или иного нарушения и операций индивидуального лица или организации.

В отчете RAPWG отмечает, что ICANN и ее различные Организации поддержки обладают определенной свободой действия в том, что касается вопросов *регистрации*, посредством разработки политики и процедур принуждения, в то время как вопросы *использования* сложнее контролировать, учитывая ограниченные полномочия ICANN в вопросе того, как владельцы доменов используют свои доменные имена. Обратите внимание, что в данном разделе представлены только те определения и виды деятельности, которые обсуждались членами RAPWG применительно к целям отчета, и не являются свидетельством ICANN в отношении того, какие виды деятельности по факту являются злоупотреблением DNS. Указанные здесь определения и виды деятельности предложены для применения в работе CCT-RT и предоставляются исключительно для информации и обсуждения.

Спецификация 11 Соглашения об администрировании новых gTLD

Спецификация 11 Соглашения об администрировании новых gTLD предписывает операторам регистратуры принимать на себя определенные обязательства по обеспечению общественных интересов (PIC) в рамках их договорных обязательств с ICANN. Подразделы 3a и 3b сосредоточены на PIC операторов регистратуры как на вопросе, связанном с злоупотреблением DNS, и описывают виды деятельности, которые следует включить в работу по сведению к минимуму и отслеживанию злоупотребляющего поведения в их TLD. Спецификация 11 гласит:¹²

3a. Оператор регистратуры включает в Соглашение между регистратурой и регистратором требование, обязывающее регистраторов включать в свои регистрационные соглашения положение, запрещающее владельцам зарегистрированных имен распространять вредоносное программное обеспечение, принимать участие в злоупотреблениях с использованием бот-сетей, заниматься фишингом, пиратством, нарушать авторские права и права на товарные знаки, вести мошенническую или вводящую в заблуждение деятельность, распространять контрафактную продукцию и вести прочую деятельность, идущую вразрез с соответствующим законодательством. Кроме того, в этом положении должны быть указаны меры пресечения (соответствующие законодательству и любым сопряженным процедурам) такой деятельности, в том числе приостановка регистрации доменного имени.

¹² “Registry Agreements,” («Соглашения об администрировании домена верхнего уровня») по состоянию на 4 февраля 2016 года, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

3b. Оператор регистратуры периодически проводит технический анализ для оценки того, не используются ли домены в TLD с целью создания таких угроз безопасности, как фарминг, фишинг, распространение вредоносного ПО и эксплуатация бот-сетей. Оператор регистратуры составляет статистические отчеты о количестве обнаруженных угроз безопасности и мерах, принятых в результате периодических проверок безопасности. Оператор регистратуры хранит такие отчеты в течение всего срока действия Соглашения, кроме случаев, когда более короткий срок предусмотрен законом или одобрен ICANN, и предоставляет их корпорации ICANN по запросу.

Виды деятельности, описанные в Спецификации 11 могут предоставить дополнительную концепцию определения для CCT-RT, поскольку они оптимизируют границы анализа.

Злоупотребление DNS: Дополнительная терминология и соображения

Стоит отметить и другие термины и соображения, касающиеся видов деятельности, составляющих злоупотребление DNS:

- **Фишинг** использует как **психологические**, так и технические средства для кражи личных идентифицирующих данных и кодов доступа к банковским счетам. Схемы психологических средств используют подставные электронные письма, призывающие пользователя посетить подложный веб-сайт и ввести финансовые данные, такие как номер кредитной карточки, имя пользователя учетной записи, пароль и номер социального страхования. **Направленный фишинг** – это особый вид махинаций, связанный с фишингом электронной почты и направленный на конкретных индивидуальных лиц, обладающих крайне важными учетными данными внутри организации, чтобы вынудить их предоставить конфиденциальную информацию.¹³
- **Fast Flux** – это технология, используемая бот-сетями при фишинге, спаме и прочей вредоносной деятельности, связанной с поставкой, при которой атаки отправляются с постоянно изменяющегося набора IP-адресов, что чрезвычайно затрудняет обнаружение.¹⁴

¹³ “SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle,” («Консультативное заключение SSAC по вопросу защиты владельцев доменов: Передовая практика сохранения безопасности и стабильности в рамках жизненного цикла управления учетными данными»)

Консультативный комитет по безопасности и стабильности ICANN, ноябрь 2015 года, <https://www.icann.org/en/system/files/files/sac-074-en.pdf>,

¹⁴ “SSAC Advisory on Fast Flux Hosting and DNS,” Консультативный комитет по безопасности и стабильности ICANN, март 2008 года, <https://www.icann.org/en/system/files/files/sac-025-en.pdf>

- **Тайпсквоттинг** — также известный как «Похищение URL» — это форма **киберсквоттинга**, рассчитанная на пользователей, делающих опечатки при вводе адреса интернет-сайта в интернет-браузер, и часто направляет пользователей на вредоносные сайты.¹⁵
- **Вредоносная реклама** – это реклама на интернет-сайте или рекламная сеть, установленная для заражения просматривающих ее вредоносным ПО либо при каждом просмотре, либо с разными интервалами, исходя из времени или количества попаданий.¹⁶
- **Отравление поисковых систем** – это деятельность, управляющая поисковыми системами для отображения результатов поиска, которые ведут на вредоносные интернет-сайты.¹⁷
- **Спуфинг-атаки** – когда злонамеренный субъект выдает себя за другое устройство или пользователя, чтобы совершить атаки на хосты сетей, украсть данные, распространить вредоносное ПО или обойти органы контроля доступа.¹⁸
- **Атаки типа «отказ в обслуживании» (DDoS)** – это кибератаки, направленные на то, чтобы сделать недоступной одну компьютерную систему или более. *Распределенная атака* – используемая посредством бот-сети – когда множество систем скоординировано, чтобы перегрузить серверы жертв запросами. Появилась новая форма **«распространенной» атаки DDoS**, которая использует отражение и распространение DNS для достижения чрезвычайно высокой скорости передачи данных для атаки (по имеющимся сведениям, превышающей 300 гигабит в секунду), которая перегружает пропускную способность сети жертвы и приводит к значительным или полным перебоям в обслуживании.¹⁹
- **Затенение доменов** – еще одна развивающаяся форма злоупотребления DNS, при которой преступники, используя

¹⁵ Moore and Edelman, “Measuring the Perpetrators and Funders of Typosquatting,” представлено на 14-й международной конференции по финансовой криптографии и защите данных, Тенерифе, январь 2010, <http://www.benedelman.org/typosquatting/typosquatting.pdf>

¹⁶ Fourth Global DNS Stability, Security, and Resiliency Symposium, Meeting Report, October 2012, <https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf>,

¹⁷ “Search Engine Poisoning,” Imperva, по состоянию на 1 февраля 2016 года, https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep

¹⁸ Veracode, “Spoofing Attack: IP, DNS & ARP,” по состоянию на 4 февраля 2016 года, <http://www.veracode.com/security/spoofing-attack>

¹⁹ “SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure,” Консультативный комитет по безопасности и стабильности ICANN, февраль 2014 года, <https://www.icann.org/en/system/files/files/sac-065-en.pdf>. Также см. Alvarez, Carlos, “Amplified DDoS Attacks: The Current Biggest Threat Against the Internet,” ICANN Blog, 11 April 2014, <https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet>

украденные или добытые фишингом учетные данные, создают множество субдоменов, ассоциирующихся с существующими законными доменами в портфеле владельца домена. С точки зрения владельца, законные домены продолжают функционировать в обычном режиме, однако эти субдомены направляют посетителей на вредоносные сайты.²⁰

- **Отравление кеша DNS** – атака, при которой злонамеренный субъект обманным путем заставляет сервер имен добавить или заменить кешированные данные DNS вредоносными данными. **Фарминг** – одна из форм этой деятельности, при которой злонамеренный субъект убеждает жертву нажать на ссылку — обычно отправленную в электронном спаме — которая, в свою очередь, заражает персональный компьютер или сервер жертвы и переадресовывает пользователей на мошеннические интернет-сайты, на которых можно собрать конфиденциальную личную информацию.²¹

Главное, о чем стоит помнить при рассмотрении всех этих тактик – это то, что они спекулируют **человеческими слабостями** в виде жадности, невнимательности и/или наивности. Таким образом, **самым слабым звеном цепи кибербезопасности, как правило, оказываются конечные пользователи.**²²

Злоупотребление DNS: Ключевая статистика и тенденции

Проведенное недавно спонсируемое ICANN глобальное исследование 6144 потребителей показало:

- 74% были осведомлены о фишинге
- 79% были осведомлены о рассылке спама
- 40% были осведомлены о киберсквоттинге
- 67% были осведомлены об украденных учетных данных
- 76% были осведомлены о вредоносном ПО




²⁰ “SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle,” («Консультативное заключение SSAC по вопросу защиты владельцев доменов: Передовая практика сохранения безопасности и стабильности в рамках жизненного цикла управления учетными данными»), Консультативный комитет по безопасности и стабильности ICANN, ноябрь 2015 года, <https://www.icann.org/en/system/files/files/sac-074-en.pdf>

²¹ См. Piscitello, Dave, “DNS Pharming: Someone’s poisoned the water hole!”, WatchGuard Technologies Expert Editorial, 2005, <http://www.corecom.com/external/livesecurity/dnsphishing.htm>

²² Khonji, Mahmoud and Youssef Iraqi, “Phishing Detection: A Literature Survey,” IEEE Communications Surveys & Tutorials 15, no. 4 (Q4 2013), doi: 10.1109/SURV.2013.032213.00009.

Наряду с высоким уровнем осведомленности о злонамеренном поведении в DNS, конечные пользователи среди потребителей сообщили о высоком уровне «сильного/некоторой степени страха» перед каждым типом злоупотребляющего поведения и продемонстрировали убеждение в том, что они являются «очень/в некоторой степени» общими.²³





Symantec, одна из крупнейших в мире компаний, занимающихся информационной безопасностью, представляет ежегодный отчет по состоянию глобальной интернет-безопасности.²⁴ В ее последнем исследовании представлено несколько индикаторов для иллюстрирования общих трендов в ключевых видах деятельности, связанных со злоупотреблением DNS. В связи с этим, данное исследование может послужить одной из отправных точек для более детального анализа злоупотреблений DNS в новых и старых gTLD по мере выполнения работы CCT-RT:

Индикатор	Описательная статистика	Тренд
Интернет-сайты с вредоносным ПО	<ul style="list-style-type: none"> • 2014: 1 из 1126 • 2013: 1 из 566 	
Общий коэффициент спама (процентная доля всех электронных писем, классифицированных как спам)	<ul style="list-style-type: none"> • 2015: 54%²⁵ • 2014: 60% • 2013: 66% 	
Глобальный объем спама в день (приблизительно)	<ul style="list-style-type: none"> • 2014: 28 миллиардов • 2013: 29 миллиардов 	

²³ Глобальное потребительское исследование, проведенное для ICANN компанией Nielsen, апрель 2015 года, <https://www.icann.org/news/announcement-2015-05-29-en>

²⁴ Symantec, “Internet Security Threat Report 20,” April 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

²⁵ Обратите внимание, что этот показатель за 2015 год взят из разведывательного отчета компании Symantec за ноябрь 2015 года на сайте www.symantec.com/content/en/us/enterprise/other_resources/intelligence-report-11-2015-en-us.pdf. Приведенный показатель представляет собой годовой показатель за вычетом показателя за декабрь 2015 года. Компания Symantec не сообщила годовых показателей за 2015 год по другим критериям, перечисленным в данной таблице.

Коэффициент фишинга электронных писем (соотношение электронных писем, которые являются попыткой осуществить фишинг)	<ul style="list-style-type: none"> • 2014: 1 из 965 • 2013: 1 из 392 	
Новые варианты вредоносного ПО, добавляемые каждый год	<ul style="list-style-type: none"> • 2014: 317 миллионов • 2013: 252 миллиона 	
Коэффициент вредоносного ПО в электронных письмах (соотношение электронных писем, содержащих вредоносное ПО)	<ul style="list-style-type: none"> • 2014: 1 из 244 • 2013: 1 из 196 • 2012: 1 из 291 	
Количество ботов	<ul style="list-style-type: none"> • 2014: 1,9 миллиона • 2013: 2,3 миллиона • 2012: 3,4 миллиона 	

Несмотря на то, что эти данные демонстрируют отрицательную динамику в конкретных формах злоупотребления DNS, важно отметить, что они представляют собой срез текущего состояния этих трендов. Например, несмотря на то, что согласно таблице число фишинговых атак снизилось, **с 2008 года количество фишинговых атак почти удвоилось**, что говорит о том, что показанная отрицательная динамика может быть ничем иным, как небольшим снижением в общей линии тренда.²⁶ Кроме того, представленные данные охватывают *всю* DNS; они не описывают конкретно злоупотребления DNS в *новых* gTLD

Злоупотребления DNS в новых gTLD

Злоупотребления DNS в новых gTLD почти не подлежали систематическому изучению, что, вероятно, связано с их новизной. Упомянутое выше спонсируемое ICANN исследование показало, что **потребительское доверие к новым gTLD намного ниже, чем к старым TLD**, где примерно 50% потребителей выразили доверие к новым по сравнению с примерно 90%, выразившими доверие к старым TLD.²⁷ Исследователи из

²⁶ Illumintel, "Potential for Phishing in Sensitive-String Top-Level Domains," study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

²⁷ Глобальное потребительское исследование, проведенное для ICANN компанией Nielsen, апрель 2015 года, <https://www.icann.org/news/announcement-2015-05-29-en>

Калифорнийского университета в Сан-Диего выяснили, что **новые домены TLD более чем в два раза чаще, чем старые TLD, попадают в черный список доменов** – список доменов известных спаммеров – в первый месяц регистрации.²⁸

Согласно мнению членов APWG, создается впечатление, что **злонамеренные субъекты проверяют пространство новых gTLD** в качестве потенциальной площадки для своей деятельности.²⁹ Они полагают, что к этому мог привести рост конкуренции на рынке новых gTLD, который вызывает снижение цен и, в свою очередь, привлекает злонамеренных субъектов, которые стремятся извлечь выгоду на фоне низких затрат. Однако они отмечают, что сделать выводы на основе ограниченных сравнительных данных – непросто, учитывая, что новые gTLD находятся на ранних этапах введения. Они предлагают провести в будущем исследования, сравнивающие злоупотребления DNS в новых и старых TLD, когда будет доступно достаточное количество данных.³⁰

Architelos, компания, занимающаяся консалтингом и управлением на рынке TLD, предлагает более детальный анализ злоупотреблений DNS в новых, старых и национальных TLD (ccTLDs). В их последнем отчете, опубликованном в июне 2015 года, используется их критерий – Индекс качества пространства имен (NQI), который представляет собой **количество злоупотребленных доменов, перечисленных в их портфеле черного списка, на миллион доменов** под управлением в каждой регистратуре, для анализа состояния злоупотребляющего поведения в старых и новых gTLD. В отчете сделано несколько важных выводов:³¹

- Согласно NQI, в период с января 2014 года по июнь 2015 года, коэффициент **злоупотреблений** (фишинг, вредоносное ПО, командование и управление бот-сетями и спам) в новых gTLD **резко вырос** с момента обнаружения первого злоупотребления в новых gTLD в феврале 2014 года, и приближается к уровням старых gTLD.

²⁸ Обратите внимание, что данный критерий представлял собой «срез», сделанный в момент проведения исследования, и не отражал долгосрочного анализа. См. Der et al., “From .academy to .zone: An Analysis of the New TLD Land Rush,” University of California, San Diego, Department of Computer Science and Engineering, October 2015, doi: 10.1145/2815675,2815696.

²⁹ Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 1H2014,” 25 September 2014, <https://apwg.org/apwg-news-center/>

³⁰ Из того же источника.

³¹ Architelos, “The NameSentrySM Abuse Report,” June 2015, <http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf>

- На долю спама приходится **99%** заявленных злоупотреблений в **новых gTLD** в течение периода проведения анализа (спам составил 90% в старых gTLD и в ccTLD).
- В мае 2015 года **показатель NQI для новых gTLD составил 11654 на миллион доменов** под управлением по сравнению с примерно **16500 на миллион в старых gTLD**
- **Кoeffициенты фишинга, вредоносного ПО и командования и управления бот-сетями в новых gTLD сохраняют чрезвычайно низкие уровни** по сравнению со старыми gTLD, хотя, вероятно, они увеличатся по мере роста осведомленности и применения новых gTLD. С мая 2014 года по май 2015 года **число «фишинговых» доменов резко выросло** с семи, обнаруженных и внесенных в черный список, до 143, 20-кратный рост (по сравнению с ростом от примерно 7300 до 14000 в старых gTLD за аналогичный период). Однако **77% из этих 143 новых сообщений о фишинге были сосредоточены всего в десяти новых gTLD.**

Анализ примеров злоупотребления DNS: Фишинг в новых gTLD

Распространение фишинга может служить одним из индикаторов того, насколько злонамеренные субъекты злоупотребляют новыми gTLD. В исследовании, соавторами которого выступили члены APWG, авторы отмечают, что **расширение DNS посредством Программы New gTLD едва ли увеличит совокупный объем фишинга в мире**, однако создаст **новые, отличные места, из которых могут проводиться фишинговые атаки**, поскольку киберпреступники склонны со временем перемещаться из одного TLD в другой.³² Фишинг-мошенники, как правило, не будут регистрировать домены, содержащие торговые названия, предпочитая вместо этого бессмысленные строки или размещение торгового названия где-то в субдомене или подпапке, поскольку владельцы торговых названий регулярно проверяют свои названия на предмет ненадлежащего использования. Во второй половине 2014 года всего 1,9% всех доменов, использовавшихся для фишинга, содержала торговое название или его вариацию (часто они были написаны с ошибкой).

В другом аналитическом исследовании, проведенном членами APWG, авторы пришли к аналогичному выводу, отметив, что новые gTLD не стали «золотой жилой» нового фишинга. Авторы обоих документов использовали критерий (« количество фишинговых доменов на 10000»), который представляет собой отношение числа доменных имен, использованных для фишинга в TLD, к числу зарегистрированных в этом TLD доменных имен в качестве способа оценки здоровья новых TLD, поскольку это относится к

³² Illumintel, “Potential for Phishing in Sensitive-String Top-Level Domains,” study for the ICANN Board of Directors New gTLD Program Committee, 21 May 2015, <https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en>

фишингу.³³ В своем анализе они пришли к выводу о том, что показатель **между 3,4 и 4,7 фишинговыми доменами на 10000 представляет собой «золотую середину» показателя распространения фишинга.**³⁴ Любой показатель выше 4,7 будет указывать на TLD с уровнями фишинга выше среднего. Средний показатель фишинговых доменов на 10000 для всех TLD во второй половине 2014 года составил 3,4. **Только девять из 295 новых gTLD (в 2014 году) обладали показателями выше 3,4.**³⁵ Кроме того, **средние показатели «оперативного времени» фишинговых атак — или того, как долго эти атаки остаются активными, и ключевой критерий устойчивости усилий фишинг-мошенников — находятся на уровне исторических минимумов, что говорит об определенных успехах в антифишинговой борьбе.**³⁶

Согласно авторам обоих документов, **стоимость домена оказывается важным определяющим стимулом фишинга** в TLD, а в старых TLD домены, как правило, стоят дешевле.³⁷ Аналогичную мысль выразило и несколько регистратур и регистраторов на спонсируемой ICANN телеконференции по измерению злоупотреблений DNS, которые отметили, что **более высокие цены на домены были ключевым фактором в сокращении злоупотреблений в целом.**³⁸ Авторы из APWG прогнозируют, что по мере распространения и снижения цен на новые gTLD ввиду роста предложения и конкуренции, мы увидим в них увеличение фишинга по сравнению со старыми и национальными TLD (ccTLD). Основное доказательство в пользу этого тренда демонстрирует пример с gTLD .xyz, который предлагал бесплатные домены в течение какого-то периода времени. Во второй половине 2014 года, почти 2/3 фишинговых атак в

³³ Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 May 2015, <https://apwg.org/apwg-news-center/>

³⁴ Обратите внимание, что отчет APWG первого полугодия 2014 года предполагал значение между 4,1 и 4,7. Эти значения изменяются, согласно «кривой» совокупной фишинговой активности.

³⁵ Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 May 2015, <https://apwg.org/apwg-news-center/>

³⁶ Во втором полугодии 2014 года *средние значения* оперативного времени немного выросли с 8 часов и 42 минут до 10 часов и 6 минут. См. Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 May 2015, <https://apwg.org/apwg-news-center/>

³⁷ Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 May 2015, <https://apwg.org/apwg-news-center/>

³⁸ Один из участников, на основе личного наблюдения, установил порог более чем в 15 долларов США за домен, когда коэффициенты злоупотребления начали падать. ICANN Operations and Policy Research, “Reviewing New gTLD Program Safeguards Against DNS Abuse,” («Анализ механизмов защиты Программы New gTLD от злоупотребления DNS»), 28 января 2016 года, материалы и записи телеконференции доступны на <https://newgtlds.icann.org/en/reviews/dns-abuse>

новых gTLD было сосредоточено в регистратуре .хуз.³⁹ Складывается впечатление, что удержание цен на низком уровне вызывает сильный интерес у фишинг-мошенников, поскольку, как показали исследования, фишинг все больше напоминает «низкооплачиваемое и не требующее особых навыков занятие».⁴⁰ Несмотря на то, что некоторые истории рассказывают о впечатляющей прибыли в результате фишинга, оказывается, что средний фишинг-мошенник может выручить порядка нескольких сотен американских долларов в неделю.⁴¹

Девять механизмов защиты

В преддверии Программы New gTLD, ICANN обратилась за консультацией к экспертам в предметной области по злоупотреблениям DNS и кибербезопасности, чтобы они предложили превентивные меры, которые можно было бы принять для сведения к минимуму описанных выше виды деятельности. Экспертное сообщество остановилось на следующих девяти механизмах защиты, представленных ниже. Теперь ССТ-RT должна определить то, насколько эффективными были эти механизмы защиты в достижении поставленных целей.

Для того чтобы понять «эффективность» девяти механизмов защиты, направленных на сведение к минимуму злоупотреблений DNS, **необходимо дать «эффективности» определение в качестве измеримого понятия.** На следующих страницах подобные определения будут обсуждаться в контексте каждого вопроса, поставленного в рамках первоначальных усилий для определения того, какие механизмы защиты были бы необходимы для Программы New gTLD. Будут представлены доступные данные по критериям «эффективности». Если данные недоступны, то последует обсуждение причин нехватки данных и других возможных способов оценки эффективности данного механизма защиты.

³⁹ Авторы отмечают, что большинство фишинговых регистраций на .хуз было совершено через китайские регистраторы и использовалось для атаки китайских целей. См. Anti-Phishing Working Group, “Global Phishing Survey: Trends and Domain Name use in 2H2014,” 27 May 2015, <https://apwg.org/apwg-news-center/>

⁴⁰ Herley and Florencio, “A Profitless Endeavor: Phishing as Tragedy of the Commons,” Microsoft Research, September 2008, <http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf>

⁴¹ Из того же источника. Учитывая «подпольную» природу, получить данные непросто. Таким образом, продолжает вестись важный спор о фактических затратах и выгодах фишинга в целом.

Вопрос: Как мы обезопасим себя от управления регистратурами недобросовестными субъектами?

В контексте данного вопроса «эффективность» можно понимать как недопущение «злонамеренных субъектов», например тех, кто осужден за тяжкое или мелкое преступление, относящееся к финансовой деятельности, к управлению регистратурами. Еще в 2001 году Соглашение об администрировании домена верхнего уровня .COM установило возможность расторжения Соглашения об администрировании домена верхнего уровня в случае, если оператор регистратуры:

«(a) был осужден судом компетентной юрисдикции за уголовное преступление или другое серьезное нарушение, относящееся к финансовой деятельности, объектом судебного постановления компетентной юрисдикции, которое ICANN обоснованно считает существенным эквивалентом любого из таковых; или
(b) государственные власти по месту жительства применяют к нему меры дисциплинарного воздействия за поведение, включающее мошенничество или нецелевое расходование денежных средств других людей».⁴²

Данное положение также присутствует в Соглашении об администрировании новых gTLD, наряду с дополнительными условиями:

(f) ICANN имеет право прекратить действие настоящего Соглашения после уведомления Оператора регистратуры, если (i) должностным лицом Оператора регистратуры является лицо, о котором известно, что оно было признано виновным в совершении правонарушения, связанного с финансовой деятельностью, или любого тяжкого преступления, признанное компетентным судом виновным в совершении мошенничества или нарушения фидуциарных обязанностей или в отношении которого вынесено решение суда, которое ICANN обоснованно считает по сути эквивалентным любому из вышеупомянутых, и отношения с данным должностным лицом не расторгнуты в течение тридцати (30) календарных дней с того момента, когда Оператор регистратуры узнал о вышеупомянутых фактах, или (ii) один из членов правления или аналогичного руководящего органа Оператора регистратуры признан виновным в совершении правонарушения, связанного с финансовой деятельностью, или любого тяжкого преступления, признан компетентным судом виновным в совершении мошенничества или нарушения фидуциарных обязанностей или в отношении него вынесено решение суда, которое ICANN обоснованно считает по сути

⁴² “.com Registry Agreement,” («Соглашение об администрировании домена верхнего уровня .com») от 25 мая 2001 года, <https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C>.

эквивалентным любому из вышеупомянутых, и отношения с данным должностным лицом не расторгнуты в течение тридцати (30) календарных дней с того момента, когда Оператор регистратуры узнал о вышеупомянутых фактах.⁴³

Механизм защиты: Проверка операторов регистратуры

История вопроса

Проверка операторов регистратуры перед заключением Соглашения об администрировании домена верхнего уровня и делегированием TLD в корневую зону добавили как механизм защиты в Руководство кандидата gTLD для Программы New gTLD, чтобы кандидаты с криминальным прошлым или злонамеренным поведением не могли управлять TLD. Данный критерий был разработан для создания регламентированного процесса отбора операторов регистратуры перед подписанием Соглашения об администрировании домена верхнего уровня в ходе первичной оценки кандидатов.

ICANN наняла PricewaterhouseCoopers (PwC) для выполнения проверки на отсутствие судимостей, сосредоточившись на двух областях: 1) общая деловая репутация и преступное прошлое, а также 2) участие в киберсквоттинге. О пригодности данного кандидата для перехода в Программу New gTLD сообщалось в отчете о первичной оценке и иногда в отчете о расширенной оценке.

Проверка на отсутствие судимостей, используемая в Программе New gTLD, проводится в процессе первичной оценки. В случаях, если кандидат вносил изменения в информацию, содержащуюся в его заявке, в процессе проведения оценки, перед подписанием Соглашения об администрировании домена верхнего уровня проводилась дополнительная проверка на отсутствие судимостей. И в каждом случае ICANN сохраняла за собой право проведения дополнительной комплексной проверки, при необходимости, перед подписанием соглашения.

Определение «эффективности»

Для данного механизма защиты, «эффективность» можно сформулировать как предотвращение заключения Соглашения об администрировании домена верхнего уровня между операторами регистратуры со злонамеренным или криминальным прошлым и ICANN. Однако, как отмечалось выше, процедура проверки осуществляется в какой-то момент времени, и в организации, ответственной за управление TLD, могут произойти изменения (например, компанию могут продать или должностное лицо может быть заменено). В контексте злоупотреблений DNS, также может оказаться важным рассмотрение вопроса о том, имеются ли

⁴³ “Registry Agreements,” («Соглашения об администрировании домена верхнего уровня») от 9 января 2014 года, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

доказательства того, что регистратурой управляет злонамеренный субъект, или имеется подобный риск, на постоянной основе.

Актуальный контекст

Согласно Отчету по реализации Программы New gTLD, опубликованному в январе 2016 года, процедура проверки на отсутствие судимостей представляла собой «анализ всех подающих заявку организаций и всех индивидуальных лиц и организаций, указанных в вопросах 9-11 заявки, включая должностных лиц и членов Правления, подающих заявку организаций, помимо акционеров, владеющих значительной долей организации».⁴⁴ Согласно отчету, ICANN провела 1150 проверок на отсутствие судимостей по 1930 заявкам (количество организаций, подавших несколько заявок). О результатах проверки на отсутствие судимостей по каждой заявке сообщалось по завершении процедур первичной оценки. В некоторых случаях комиссия, проводящая проверку на отсутствие судимостей, задавала кандидатам уточняющие вопросы. В целом, в Отчете по реализации Программы New gTLD проверка на отсутствие судимостей была названа успешной, поскольку удалось проверить всех кандидатов, однако отмечалось, что период между крайним сроком подачи заявки и подписанием Соглашений об администрировании домена верхнего уровня оказался дольше ожидаемого. Это означает, что многих кандидатов пришлось проверять повторно. В отчете предлагается проводить проверку на отсутствие судимостей на этапе заключения договора, а не во время первичной оценки, чтобы свести к минимуму потребность в повторной проверке.

Возможные методы сбора и измерения данных

Возможно, еще слишком рано, чтобы определить, оба ли аспекта этого механизма защиты были настолько же эффективными, как и превентивные меры. Любой критерий «эффективности» должен учитывать данные по отказам, исходя из первичной проверки на отсутствие судимостей, а также по расторжениям Соглашений об администрировании домена верхнего уровня ввиду того, что регистратура не смогла исключить злонамеренные субъекты из должностных лиц или Правления. Из-за включенной личной информации и конфиденциальности в вопросе проверки на отсутствие судимостей, отчеты, указывающие на пригодность кандидатов к переходу на следующий этап процедуры, ограничены. Однако доступны совокупные показатели. Официальные жалобы на соответствие и/или расторжения Соглашений об администрировании домена верхнего уровня могут послужить способом оценки того, остается ли данный механизм защиты эффективным.

Кроме того, возможно, данный механизм защиты оказал сдерживающее воздействие на потенциальных кандидатов с персоналом, чье прошлое не

⁴⁴ “Program Implementation Review,” 29 January 2016, <https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf>

внушает доверия. Тем не менее, измерить сдерживающее воздействие – т. е. сколько кандидатов *не* подали заявку – практически невозможно, учитывая, что подобное воздействие не формирует измеряемых данных.

Вопрос: Как мы обеспечим целостность и полезность информации о регистратуре?

Определение «эффективности» в рамках данного вопроса можно понимать как успешное использование механизмов защиты для оказания помощи в проверке и обеспечении безопасности информации о регистратуре. Для этого были разработаны следующие три превентивных механизма защиты.

Механизм защиты: Требовать демонстрацию плана по развертыванию DNSSEC

История вопроса

Расширение безопасности системы доменных имен (DNSSEC) было создано для сокращения со стороны злонамеренных субъектов числа попыток взлома процедуры поиска DNS. Такие субъекты могут взломать поисковые запросы интернет-пользователя и, например, направить его на вредоносные веб-сайты, чтобы украсть конфиденциальную информацию. DNSSEC защищает от таких атак с помощью цифровой подписи данных, которая позволяет быть уверенным в их достоверности. Оно использует криптографические подписи к существующим записям DNS для проверки того, что запись DNS исходит от официального сервера имен и не была изменена ни в один момент.⁴⁵ Развертывание регистратур DNSSEC позволяет владельцам доменов по желанию присваивать специальные ключи доменных имен к своим доменам. Установление DNSSEC в качестве обязательного посредством Соглашения об администрировании домена верхнего уровня было направлено на обеспечение его более обширного и быстрого развертывания.

Данный механизм защиты требует, чтобы у всех кандидатов на новый gTLD был конкретный план по развертыванию DNSSEC. Он оценивается в процессе первичной оценки, главная задача состоит в сокращении риска получения подставных записей DNS. Согласно Соглашению об администрировании домена верхнего уровня, операторы регистратуры новых gTLD обязаны подписывать файлы корневой зоны TLD с помощью DNSSEC, руководствуясь передовой практикой, как описано в RFC 4641 Инженерной проектной группы интернета (IETF) и ее преемниками, принимать данные с открытым ключом от дочерних доменных имен

⁴⁵ “DNSSEC – What Is It and Why Is It Important?” по состоянию на 1 февраля 2016 года, <https://www.icann.org/resources/pages/dnssec-qa-2014-01-29-en>; “How DNSSEC Works,” по состоянию на 1 февраля 2016 года, <https://www.cloudflare.com/dnssec/how-dnssec-works/>

безопасным образом и публиковать положения о практике DNSSEC (DPS) в соответствии с форматом, указанным в RFC 6841.^{46 47}

Определение «эффективности»

«Эффективность» данного механизма защиты можно определить несколькими способами. Ее можно определить просто как наличие у оператора регистратуры конкретного плана по развертыванию DNSSEC, и прохождение проверки на этапе подачи заявки. Ее также можно определить в соответствии с числом проблем, заявленных в отношении соответствия регистратуры требованиям DNSSEC. И наконец, ее можно определить в соответствии с более обширным распространением DNSSEC, например, коэффициент подписей, сделанных владельцами доменов или разработка преобразователей DNS, проверяющих DNSSEC, внутри сетей, управляемых интернет-провайдерами (ISP).⁴⁸

Актуальный контекст

На 23 февраля 2016 года 1073 из 1236 TLD (включая ccTLD) в корневой зоне имели ключи подписи DNSSEC.⁴⁹

Возможные методы сбора и измерения данных

Двумя доступными на данный момент способами измерения являются: число TLD в корневой зоне и число доменов второго уровня в каждом домене с ключами подписи.⁵⁰ Более углубленные критерии могли сосредоточиться на измерении проблем DNSSEC, с которыми пришлось столкнуться во время тестирования функциональности перед запуском, на количестве проблем мониторинга Соглашения об уровне обслуживания (SLA), о которых было сообщено, и на числе жалоб, полученных в отношении соблюдения обязательств DNSSEC.

⁴⁶ ICANN Registry Agreement, Specification 6: 1.2 DNSSEC («Соглашение об администрировании домена верхнего уровня ICANN, Спецификация 6: 1.2 DNSSEC»), по состоянию на 1 февраля 2016 года,

<https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>

⁴⁷ «RFC» – это созданный IETF набор документации «Запрос комментариев», который содержит технические и организационные инструкции по построению компьютерных сетей, протоколам, процедурам и понятиям. См. www.ietf.org/rfc

⁴⁸ «Deployment Guide: DNSSEC for Internet Service Providers (ISPs),» по состоянию на 1 февраля 2016 года, <http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/>

⁴⁹ «TLD DNSSEC Report,» по состоянию на 23 февраля 2016 года, http://stats.research.icann.org/dns/tld_report/

⁵⁰ См. «DNSSEC Deployment Report,» по состоянию на 23 февраля 2016 года, <http://rick.eng.br/dnssecstat/>

Всестороннему критерию «эффективности» в этой области придется учитывать тот факт, что регистраторы, владельцы доменов, провайдеры хостинга DNS и ISP – все они играют главную роль в полном развертывании и функциональных возможностях DNSSEC. Например, несмотря на то, что владельцы доменов обязаны продемонстрировать план развертывания DNSSEC, это не означает, что владельцы доменов обязательно зарегистрируются. Предварительные данные, собранные технической службой ICANN, указывают на то, что лишь небольшой процент доменов второго уровня имеет ключи подписи DNSSEC (хотя это сильно различается в зависимости от TLD).⁵¹ Возможным примером для рассмотрения может стать ситуация с CloudFlare — компанией, осуществляющей обслуживание серверов доменных имен и предоставляющей услуги по доставке контента DNS — которая решила позволить любому в своей сети защитить свой трафик с помощью DNSSEC в один прием. Подход с анализом примеров, который обеспечивает межотраслевой взгляд на поддержку DNSSEC, оказываемую регистратурами, регистраторами, провайдерами хостинга DNS и ISP, может дать возможность идентифицировать слабые места в развертывании DNSSEC по всем gTLD. Группой, уже собирающей такую информацию, является Рабочая группа по развертыванию DNSSEC, которая выкладывает отчеты на dnsssec-deployment.org.

Механизм защиты: Запрет на использование символов обобщения имени

История вопроса

Данная рекомендация требует соответствующих мер защиты от использования «символов обобщения имени» в DNS. Речь идет о том, когда вместо предоставления ответа «ошибка имени» для несуществующих запросов DNS, оператор регистратуры использует переадресацию DNS, символы обобщения имени или синтезированные ответы.⁵² ICANN запретила эти действия ввиду полученных результатов, показавших, что такие действия несут в себе угрозу безопасности и стабильности DNS путем создания новых возможностей для злонамеренных атак.⁵³

Определение этому механизму защиты дано в разделе 2.2 Спецификации 6 к Соглашению об администрировании домена верхнего уровня:

⁵¹ Данные, собранные технической службой ICANN в общеизвестных файлах корневой зоны в целях этого отчета.

⁵² “About Wildcard Prohibition (Domain Redirect),” по состоянию на 1 февраля 2016 года, <https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en>

⁵³ Консультативный комитет по безопасности и стабильности ICANN, “SAC041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs,” 10 June 2009, <https://www.icann.org/en/system/files/files/sac-041-en.pdf>

2.2. Запрет на использование символов обобщения имени. Для доменных имен, которые еще не зарегистрированы или в отношении которых владельцы регистраций не предоставили допустимые записи (напр., записи серверов имен NS) для включения в список файла корневой зоны DNS или для доменных имен, которые не могут быть опубликованы в DNS в силу своего статуса, не допускается использование Оператором регистратуры в DNS записей ресурсов с символами обобщения имени (символами замещения), как описано в документах RFC 1034 и 4592, а также любых других технологий и методов синтеза записей ресурсов DNS или переадресации внутри DNS. При получении запросов на разрешение таких доменных имен полномочные серверы имен должны выводить сообщение: «Name Error» («Ошибка имени» или NXDOMAIN), RCODE 3, как описано в RFC 1035 и связанных с ним RFC. Это относится ко всем файлам корневой зоны DNS на всех уровнях дерева DNS, в отношении которых Оператор регистратуры (или аффилированное с ним лицо, занимающееся оказанием Услуг регистрации) хранит данные, организует такое хранение данных или получает прибыль от такого хранения.

Однако в 2014 году, в составе Рамочного плана действий в случаях совпадения имен, символы обобщения имени использовались в некоторых TLD в течение ограниченного периода времени, сразу после делегирования TLD (период управляемого прерывания) в качестве средства идентификации любых совпадений в пространстве имен.⁵⁴ Как указано в Отчете JAS о первом этапе – *Снижение риска совпадений в пространстве имен DNS*:

Мы рекомендуем регистратуре ввести период управляемого прерывания незамедлительно после делегирования в корневой зоне и временно приостановить запрет на записи с символами обобщения

⁵⁴ См. “Frequently Asked Questions: Name Collision Occurrence Management Framework for Registries,” по состоянию на 11 февраля 2016 года, www.icann.org/resources/pages/name-collision-ro-fags-2014-08-01-en, где указано: «Запрет на использование символов обобщения имени не распространяется на период управляемого прерывания для соответствующих TLD (например, если нет активных имен в TLD, за исключением «nic»). Разрешение на отступление от требования действует, только если нет делегированных (а значит, работающих) имен в данном TLD, что устраняет риски, обычно связанные с использованием символов обобщения имени. Причиной отмены запрета и использования символов обобщения имени является необходимость опробовать все ситуации очевидных конфликтов имен. Символ обобщения имени в «верхней» части зоны будет соответствовать всем запросам, которые будут отображаться при запуске зоны в работу. Такой подход позволяет использовать все меры для защиты интернет-пользователей, которые в настоящее время направляют в глобальную сеть запросы, обращенные к локальной сети».

имени на этот период. Учитывая цель управляемого прерывания и тот факт, что в этот момент в зоне не будет никаких данных о владельце домена, мы полагаем, что временное разрешение использовать в записях символы обобщения имени с этой целью, не противоречит установленным ICANN запретам по записям с символами обобщения имени и не вызывает волнений, которые привели ICANN к установке этих запретов.⁵⁵

Определение «эффективности»

Для данного критерия «эффективность» теоретически можно определить с учетом соблюдения запрета на использование символов обобщения имени в новых gTLD. Также можно рассмотреть оценку данного поведения в качестве способа обеспечения целостности и полезности информации регистратуры. Также можно оценить вклад, который стремился внести этот механизм защиты в оказание влияния на поведение.

Актуальный контекст

ICANN открывает доступ к «Бланку жалоб на Запрет на символы обобщения имени (переадресация домена)» для предоставления отчетов о несоблюдении положений договора.⁵⁶ На сегодняшний день ICANN не получила ни одной жалобы на запрет использования символов обобщения имени посредством этого инструмента.⁵⁷

Возможные методы сбора и измерения данных

Как указано выше, в отношении использования символов обобщения имени регистратурами новых gTLD не было получено ни одной жалобы. Качественное исследование эффективности данного механизма защиты совместно с экспертами в предметной области может помочь компенсировать нехватку количественных данных.

Другой подход может включать в себя не только рассмотрение поступивших в ICANN жалоб о недостатках запрета на символы обобщения имени в конкретных TLD, но и текущее преобладание использования переадресации

⁵⁵ JAS Global Advisors, “Mitigating the Risk of DNS Namespace Collisions,” 4 June 2014, <https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf>

⁵⁶ См. “Wildcard Prohibition (Domain Redirect) Complaint Form,” по состоянию на 11 февраля 2016 года, <https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form>

⁵⁷ Тем не менее, отдел соблюдения договорных обязательств получил несколько жалоб в отношении «Зарезервированных имен/Управляемого прерывания». См. “ICANN Contractual Compliance Dashboard for 2016,” по состоянию на 12 февраля 2016 года, <https://features.icann.org/compliance/dashboard/0116/report>

DNS для «монетизации ошибочного трафика», которая заключается в DNS-переадресации пользователей на рекламоориентированные интернет-серверы, когда их DNS-поиск не удается. Созданный в ICSI Калифорнийского университета в Беркли Netalyzr – это инструмент диагностики сети, также входящий в состав измерительного исследования, направленного на измерение здоровья интернета. Он использовался в предыдущих исследованиях, изучающих проблемы DNS-переадресации, и может быть полезным для понимания последствий использования символов обобщения имен в DNS.⁵⁸

Механизм защиты: Удаление потерянных связующих записей

История вопроса

Этот механизм защиты был разработан, чтобы сократить риск скрытого внедрения злонамеренными субъектами ссылок на вредоносные домены в корневой зоне посредством «потерянных связующих» записей, которые могут сохраняться после удаления «родительской» записи из зоны. Потерянные связующие записи позволяют злонамеренным субъектам получить управление серверами имен, что затем дает им возможность осуществлять вредоносную деятельность с доменов, которые на первый взгляд кажутся «законными». Например, известно, что атаки с помощью технологии Fast Flux используют потерянные связующие записи для хостинга вредоносных доменов в течение короткого периода времени.⁵⁹

Этот механизм защиты требует, чтобы операторы регистратуры предоставляли в своих заявках план по удалению потерянных связующих записей после удаления родительской записи. Связанные условиями Соглашения об администрировании домена верхнего уровня, операторы регистратуры должны принимать меры по удалению потерянных связующих записей в соответствии с разделом 4.2 спецификации 6 Соглашения, который гласит: «Операторы регистратуры обязуются принимать меры для удаления потерянных связующих записей... в случае представления письменных доказательств того, что такие потерянные записи связаны со злонамеренным поведением».⁶⁰

Определение «эффективности»

Для этого критерия «эффективность» может пониматься как упорядоченная практика со стороны регистратур, состоящая в предоставлении контактной

⁵⁸ Weaver, Kreibich, and Paxson, “Redirecting DNS for Ads and Profit,” USENIX Workshop on Free and Open Communications on the Internet (FOCI), 2011, <http://www.icir.org/christian/publications/2011-foci-dns.pdf>

⁵⁹ См. Консультативный комитет по безопасности и стабильности ICANN, “SSAC Advisory on Fast Flux Hosting and DNS,” март 2008 года, <https://www.icann.org/en/system/files/files/sac-025-en.pdf>

⁶⁰ См. Консультативный комитет по безопасности и стабильности ICANN, “SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook,” May 2011, <https://www.icann.org/en/system/files/files/sac-048-en.pdf>

информации конечным пользователям для сообщения о злоупотреблении и подтверждении автоматического удаления потерянных связующих записей при удалении родительской записи из зоны.

Актуальный контекст

Первоначальная обратная связь от сообщества предполагает, что потерянные связующие записи как источник злоупотреблений, по большей части, были нейтрализованы посредством регулярной практики удаления их из файлов корневой зоны, хотя в некоторых случаях они остаются проблемой «низкого уровня».⁶¹

Возможные методы сбора и измерения данных

Полученная ICANN первоначальная обратная связь содержала несколько предложений о том, чтобы этот механизм защиты измерялся путем использования файлов корневой зоны для отслеживания удаления потерянных связующих записей спустя некоторое время.

Обсуждение распространения и использования потерянных связующих записей в злонамеренных целях вместе с операторами регистратуры может представить качественный показатель эффективности использования регистратурами, регистраторами и владельцами доменов требуемых механизмов для удаления потерянных связующих записей. «Письменные доказательства», требуемые от операторов регистратуры для удаления потерянных связующих записей, согласно требованиям Спецификации 6, также могут обеспечить полезный источник данных. Они также могут оказаться полезными для определения местоположения примеров рекомендаций по удалению потерянных связующих записей в политике противодействия злоупотреблениям регистратурами. Например, TLD «.rich» включает раздел, посвященный удалению потерянных связующих записей, в свою политику противодействия злоупотреблениям,⁶² в то время как Afilias фокусируется на проблеме как на элементе хостинга с технологией Fast Flux.⁶³

⁶¹ ICANN Operations and Policy Research, “Reviewing New gTLD Program Safeguards Against DNS Abuse,” («Анализ механизмов защиты Программы New gTLD от злоупотребления DNS»), 28 января 2016 года, материалы и записи телеконференции доступны на

<https://newgtlds.icann.org/en/reviews/dns-abuse>

⁶² “.RICH Anti-Abuse Policy,” по состоянию на 11 февраля 2016 года,

<http://nic.rich/files/policies/rich-anti-abuse-policy.pdf>

⁶³ “Afilias Anti-Abuse Policy,” по состоянию на 11 февраля 2016 года,

<http://dotblue.blue/about/afilias-anti-abuse-policy>

Вопрос: Как мы обеспечим более целенаправленную работу по борьбе с идентифицированным злоупотреблением?

Данный вопрос сосредоточен на доступности информации, позволяющей предотвратить деятельность недобросовестных пользователей и способствовать определению местоположения идентифицированного недобросовестного пользователя в DNS.

Механизм защиты: Требование записей централизованного WHOIS

История вопроса

Данный механизм защиты требует, чтобы новые gTLD поддерживали и обеспечивали доступ к «записям централизованного WHOIS» в целях улучшения доступности и полноты данных WHOIS. Записи централизованного WHOIS – это записи, принадлежащие регистратурам, которые «содержат контактную информацию владельца доменного имени и предусмотренную контактную информацию лица по техническим вопросам, помимо спонсирующего регистратора и состояния регистрации».⁶⁴ Они отличаются от записей «сокращенного варианта данных WHOIS», которые хранят только информацию, необходимую для идентификации спонсирующего регистратора и состояния регистрации, и не предоставляют никакой информации о владельце домена. Использование записей централизованного WHOIS может создать возможность более полного и быстрого поиска данных во время попытки идентифицировать злонамеренные субъекты, действующие в DNS.

Определение «эффективности»

Для этого критерия «эффективность» может определяться разработкой набора записей централизованного WHOIS, которые регулярно используются властями для отслеживания, идентификации и предотвращения деятельности злонамеренных субъектов в DNS.

Актуальный контекст

Каждый оператор регистратуры новых gTLD, который делегировал свои TLD в корневую зону, обязан создавать и сохранять записи в централизованном WHOIS в рамках договорных обязательств.

Возможные методы сбора и измерения данных

Намерение, стоящее за введением обязательного сохранения регистратурами новых gTLD записей в централизованном WHOIS, заключалось в создании более универсального набора контактных записей, которые позволили бы властям отслеживать и останавливать злонамеренную деятельность. Получение обратной связи от ответчиков злоупотребленных DNS о пользе записей централизованного WHOIS по

⁶⁴ ICANN WHOIS, “WHOIS Primer,” по состоянию на 11 февраля 2016 года, <https://whois.icann.org/en/primer>

сравнению с сокращенным вариантом данных WHOIS для предотвращения злоупотребления DNS может стать одним из способов оценки эффективности этого механизма защиты.

Другие потенциальные критерии могут брать начало в данных, создаваемых системой учета достоверности данных (ARS) WHOIS, которая находится сейчас в разработке и чья цель заключается в том, чтобы «систематически идентифицировать и сообщать о достоверности для повышения качества контактных данных в WHOIS». ⁶⁵ Следующие графики из отчета об этапе 2, опубликованного в декабре 2015 года, подводят итог общей достоверности данных gTLD, согласно требованиям Соглашения об аккредитации регистраторов (RAA) 2009 к синтаксису в разрезе видов связи, и общей достоверности данных gTLD, согласно требованиям RAA 2009 к функциональной пригодности в разрезе видов связи:⁶⁶

Общая достоверность данных gTLD, согласно требованиям RAA 2009 к синтаксису в разрезе видов связи

	Электронная почта	Телефон	Почтовый адрес	ВСЕ 3 достоверны
ВСЕ 3 контакта достоверны	99,1% ±0,2%	83,3% ±0,7%	79,4% ±0,8%	67,2% ±0,9%

Общая достоверность данных gTLD согласно требованиям RAA 2009 к функциональной пригодности по виду связи

	Электронная почта	Телефон	Почтовый адрес	ВСЕ 3 достоверны
ВСЕ 3 контакта достоверны	87,1% ±0,7%	74,0% ±0,9%	98,0% ±0,3%	64,7% ±0,9%

⁶⁵ Обратите внимание, что этап 3 исследования еще только предстоит пройти, но он будет сосредоточен на «Требованиях к идентифицирующим данным», которые проверяют, является ли предоставленный контакт индивидуальным лицом или организацией, ответственной за домен. «Требования к синтаксису» определены как формат записи в WHOIS. «Требования к функциональной пригодности» определены как способность контактов решать и подключаться к пользователю. Обратите внимание, что несмотря на то, что контакты могут быть функционирующими и подключаться к пользователю, ARS не проверяет пользователя на соответствие тому, что указан в записи в WHOIS. См. "WHOIS ARS Phase 2 Cycle 1 Report: Syntax and Operability Accuracy," по состоянию на 1 февраля 2016 года, <https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy> и "WHOIS Accuracy Reporting System (ARS)," по состоянию на 11 февраля 2016 года, <https://whois.icann.org/en/whoisars>

⁶⁶ Из того же источника.

Три этапа исследования ARS в WHOIS – которое концентрируется на синтаксисе, достоверности и действительности, соответственно – могут обеспечить набор репрезентативных данных для эффективности этого механизма защиты. Теоретически, более достоверные записи в WHOIS обеспечат сообщество, оказывающее противодействие злоупотреблениям, полезным инструментом для борьбы со злоупотреблением DNS. Тем не менее, едва ли злонамеренные субъекты предусмотрительно выдадут «достоверную» контактную информацию. Теперь CCT-RT должна определить, являются ли синтаксис, достоверность и действительность подходящими индикаторами для определения эффективности в этой области.

Механизм защиты: Централизация доступа к файлам зон

История вопроса

Для данного механизма защиты необходимо, чтобы параметры доступа для получения данных о файле корневой зоны регистратуры были доступны посредством централизованного источника, что позволяет противодействующему злоупотреблениям сообществу более эффективно получать обновления по новым доменам по мере их создания в каждой зоне TLD. Это направлено на сокращение времени, необходимого для принятия мер по устранению в TLD, в котором ведется злонамеренная деятельность.

Определение «эффективности»

Для данного механизма защиты, «эффективность» может означать способность Централизованной службы файлов корневой зоны (CZDS) своевременно и эффективно обрабатывать запросы для данных файла зоны регистратуры, чтобы свести к минимуму скорость противостояния злонамеренной деятельности.

Актуальный контекст

Регистратуры новых gTLD должны (согласно разделу 2 Спецификации 4 Соглашения об администрировании домена верхнего уровня) предоставлять данные зоны тем конечным пользователям, которые их запросят. Согласно находящимся в открытом доступе отчетам ICANN, только в 2015 году было утверждено более 3 миллионов паролей для доступа к файлу корневой зоны (ZFA).⁶⁷ Согласно проведенным в целях данного отчета беседам с исследователями безопасности, CZDS является чрезвычайно важной службой для ответчиков злоупотребленных DNS и для тех, кто стремится защитить свою интеллектуальную собственность. Тем не менее, несмотря на то, что CZDS была разработана с целью повышения эффективности процесса предоставления доступа к файлам корневой

⁶⁷ CZDS ZFA- Password Monthly Reports, по состоянию на 1 февраля 2016 года, <https://czds.icann.org/en/reports>

зоны, сами регистратуры выражали повсеместное недовольство этой службой.⁶⁸ Операторы регистратуры по-прежнему вынуждены проверять достоверность конечного пользователя, а Соглашение об администрировании домена верхнего уровня не ограничивает время, в течение которого операторы регистратуры должны отвечать на запросы доступа. В результате у операторов регистратуры часто «накапливается» неконтролируемое количество запросов и отсутствует возможность своевременного ответа на запросы. Один из представителей регистратур сообщил о получении 7000-10000 запросов на доступ к файлу корневой зоны *в день*.⁶⁹ Это может привести к неполному соблюдению правил пользования и поверхностной проверке подлинности учетных данных инициатора запроса.⁷⁰ Отдел соблюдения договорных обязательств ICANN назвал запросы на предоставление третьим лицам доступа к файлу корневой зоны посредством CZDS одной из главных проблем соблюдения обязательств регистратурами на 2015 год, где большинство жалоб было связано с тем, что операторы регистратуры не отвечали на запросы на получение доступа к файлу корневой зоны и отказывали в доступе по причинам, не указанным в Соглашении об администрировании домена верхнего уровня.⁷¹

Возможные методы сбора и измерения данных

Возможный приблизительный показатель «эффективности» можно измерить с помощью отчетов о паролях CZDS, демонстрирующих количество паролей ZFA (выданных в общем объеме пользователям, запросившим доступ к файлам корневой зоны) внутри CZDS и число паролей, одобряемых каждый месяц внутри конкретных TLD и в целом.⁷² Обратная связь от пользователей может обеспечить дополнительную информацию о подобном критерии, поскольку многие пользователи сообщают о проблемах, связанных с обработкой запросов CZDS, по крайней мере, на основе личного наблюдения.

⁶⁸ ICANN Operations and Policy Research, “Reviewing New gTLD Program Safeguards Against DNS Abuse,” («Анализ механизмов защиты Программы New gTLD от злоупотребления DNS»), 28 января 2016 года, материалы и записи телеконференции доступны на <https://newgtlds.icann.org/en/reviews/dns-abuse>

⁶⁹ Из того же источника.

⁷⁰ Из того же источника.

⁷¹ “ICANN Contractual Compliance 2015 Annual Report,” January 2016, <https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf>

⁷² CZDS ZFA- Password Monthly Reports, по состоянию на 1 февраля 2016 года, <https://czds.icann.org/en/reports>

Механизм защиты: Документальное оформление контактов и процедур по вопросам злоупотреблений на уровне регистратур

История вопроса

Данный механизм защиты требует от операторов регистратур наличия единого контактного лица, ответственного за рассмотрение жалоб на злоупотребления. В Руководстве кандидата указано, что кандидаты должны разработать «план реализации для назначения и размещения на своем веб-сайте единого контактного лица по вопросам злоупотреблений; это контактное лицо будет отвечать за разрешение проблем, требующих немедленного вмешательства, и за своевременное решение жалоб, касающихся злоупотреблений».⁷³ Раздел 4.1 Спецификации 6 Соглашения об администрировании домена верхнего уровня гласит: «Оператор регистратуры обязуется сообщить ICANN и опубликовать на своем веб-сайте свои точные контактные данные, включая действующий адрес электронной почты и почтовый адрес, а также основное контактное лицо, отвечающее за обработку запросов, касающихся злонамеренного поведения в данном TLD; он обязан также незамедлительно уведомлять ICANN о любых изменениях таких контактных данных».⁷⁴

Определение «эффективности»

Показателем «эффективности» данного критерия могла бы стать доступность этой информации для пользователей интерфейса и нахождение способа измерения относительной простоты подачи пользователями отчетов о злоупотреблении DNS. Вспомогательным методом мог бы послужить опрос сотрудников правоохранительных органов и самих операторов регистратур для получения от них обратной связи по вопросу эффективности данного критерия.

Актуальный контекст

Отдел соблюдения договорных обязательств ICANN отслеживал контактные сведения для борьбы со злоупотреблениями, которые регистратуры обязаны публиковать на своих веб-сайтах, и для анализа проблемы в последнем отчете отдела соблюдения договорных обязательств сказано:

ICANN продолжила проводить упреждающий мониторинг наличия контактных данных для сообщений о нарушениях, которые регистратуры обязаны размещать на своих веб-сайтах, согласно Новому соглашению об администрировании домена верхнего уровня. Тем самым, ICANN следит за тем,

⁷³ “gTLD Applicant Guidebook,” 4 June 2012, <https://newgtlds.icann.org/en/applicants/agb>

⁷⁴ “Registry Agreements,” («Соглашения об администрировании домена верхнего уровня») от 9 января 2014 года, <https://www.icann.org/resources/pages/registries/registries-agreements-en>

чтобы конечные пользователи, включая правоохранительные органы, но не ограничиваясь ими, могли связаться с регистратурой для уведомления о вредоносной деятельности в TLD... ICANN проверила веб-сайты 64 доменов верхнего уровня, период требований для которых начался между 1 января 2015 года и 31 марта 2015 года. Количество запросов или уведомлений о несоблюдении, направленных в адрес регистратур, было меньше, чем в предыдущем контрольном цикле. Среди прочего, были отмечены следующие недостатки: отсутствие отображения всей необходимой информации; отсутствие данных основного контактного лица или отсутствие почтового адреса для сообщения о нарушениях. ICANN проводит совместную работу с регистратурами по устранению обнаруженных проблем, связанных с несоблюдением обязательств.⁷⁵

Первоначальная обратная связь от сообщества в отношении этого механизма защиты отчасти указывает на то, что контактные лица, указанные для вопросов злоупотребления, в основном, использовались спаммерами.⁷⁶

Возможные методы сбора и измерения данных

Анализ отчетов отдела соблюдения договорных обязательств ICANN и отзывов тех, кто использует эти контакты, может стать способом измерения эффективности данного механизма защиты. Другой метод может предусматривать сбор контактных данных регистратур для сообщений о злоупотреблениях и проверку их работоспособности.

Механизм защиты: Участие в процедуре запроса на срочное обеспечение безопасности регистратуры (ERSR)

История вопроса

Данный механизм защиты дает операторам регистратуры возможность принимать быстрые и решительные меры в свете системных угроз DNS путем создания специальной процедуры срочного рассмотрения и санкционирования запросов о безопасности. На практике, регистратуры могут запросить оговоренное в соглашении разрешение на отступление от требования, которое освободит их от выполнения требований конкретного положения в Соглашении об администрировании домена верхнего уровня

⁷⁵ См. "ICANN Contractual Compliance Update January – March 2015," <https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf>.

⁷⁶ ICANN Operations and Policy Research, "Reviewing New gTLD Program Safeguards Against DNS Abuse," («Анализ механизмов защиты Программы New gTLD от злоупотребления DNS»), 28 января 2016 года, материалы и записи телеконференции доступны на <https://newgtlds.icann.org/en/reviews/dns-abuse>

на период, необходимый для реагирования на угрозу безопасности. Оно было создано для предоставления операционной безопасности от угрозы и одновременного уведомления соответствующих сторон о состоянии угрозы. Обратите внимания, что эта процедура была введена в ответ на вирус Conficker, а значит – до проведения работы по определению механизмов защиты для Программы New gTLD. Она не включена в последнюю версию Соглашения об администрировании домена верхнего уровня, однако в качестве процедуры доступна регистраторам, которые явно и очевидно в ней нуждаются.⁷⁷

Определение «эффективности»

«Эффективность» можно себе представить как скорость, с которой была идентифицирована и нейтрализована угроза безопасности в результате ERSR.

Актуальный контекст

С учетом того, что используемые данные требуют особого внимания, ICANN не разглашает подробности данной процедуры. Согласно начальным данным, полученным от исследователей безопасности в целях данного отчета, этот механизм защиты эффективно применялся с момента появления вируса Conficker для уничтожения последующих бот-сетей.

Возможные методы сбора и измерения данных

Для осознания эффективности данного критерия, можно получить обратную связь от тех, кто запрашивал процедуру ERSR, чтобы понять ее способность обращаться с угрозами безопасности. Учитывая ограниченное количество запросов на ERSR, а также тот факт, что связанные с безопасностью данные, присущие этой процедуре, требуют особого внимания, можно сосредоточить аналитическое внимание на том, как выполнялась эта процедура — например, скорость и относительная простота устранения угрозы в результате ERSR — а не на количестве примеров запроса ERSR или подробностях того, как угрозе безопасности было оказано противодействие.

Вопрос: Как мы обеспечим улучшенную концепцию управления для TLD с внутренним потенциалом злонамеренного поведения?

Механизм защиты: Создать проект концепции для программы проверки зон с высокой степенью безопасности

История вопроса

Данная *рекомендация* — это не было ни формально закреплено в Соглашении об администрировании домена верхнего уровня в качестве обязательного механизма защиты, ни установлено в качестве

⁷⁷ “Registration Abuse Policies Working Group Final Report,” May 2010, <http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf>

официальной, поддерживаемой ICANN инициативы — предполагала создание добровольной программы для операторов регистратуры, которые хотели установить и подтвердить повышенный уровень безопасности и надежности в своих TLD. Общая цель программы заключалась в предоставлении стандартизированного набора действий для регистратур, пытающихся выделить себя среди этих строк.⁷⁸

Определение «эффективности»

Для данного критерия, «эффективностью» можно считать успешное применение, реализацию и проверку зон с высокой степенью безопасности (HSZ) в TLD с высокой вероятностью злоупотребления (например, TLD, представляющие банковский/финансовый и фармацевтический секторы).

Актуальный контекст

Несмотря на то, что всесторонний проект концепции для такой программы так и не был официально оформлен посредством различных механизмов разработки политики и реализации ICANN, ряд усилий был направлен на изучение роста потребностей в конкретных строках в области безопасности.

Во время процесса рассмотрения заявок на новые gTLD оценивалась политика обеспечения безопасности кандидатов, поскольку она связана со строками, требующими повышенного внимания, согласно общим положениям вопроса 30 Руководства кандидата, которые требуют, чтобы кандидаты

...предоставляли краткий обзор своей политики обеспечения безопасности для предлагаемой регистратуры, включая, но не ограничиваясь...[a] описанием расширенных уровней безопасности или возможностей, соответствующих природе, применимой к строке TLD, в том числе указание на существующие международные или отраслевые стандарты безопасности, которым кандидат намерен следовать...⁷⁹

Кроме того, Правительственный консультативный комитет ICANN рекомендовал создать модель для проверки и подтверждения учетных данных оператора регистратуры в качестве обязательств по обеспечению общественных интересов (PIC) в высокорегулируемых секторах, чтобы установить и поддерживать благонадежность этих доменов.⁸⁰

⁷⁸ icann.org, “Public Comment: High Security Zone TLD Final Report,” 11 March 2011, <https://www.icann.org/news/announcement-2011-03-11-en>

⁷⁹ “gTLD Applicant Guidebook,” 4 June 2012, <https://newgtlds.icann.org/en/applicants/agb>

⁸⁰ См. “GAC Communiqué – Buenos Aires, Argentina,” 24 June 2015, <https://www.icann.org/news/announcement-2-2015-06-24-en> и “GAC Communiqué - Dublin, Ireland,” 21 October 2015, <https://www.icann.org/news/announcement-2015-10-22-en>

Также со стороны отраслевых объединений и регистратур был предпринят ряд независимых усилий по усилению безопасности и надежности в новых gTLD. Например, fTLD Registry Services LLC проводит независимую работу по установке зоны с повышенной безопасностью для собственных TLD «.bank» и «.insurance».⁸¹ Проект «DNS Seal Project» работает над созданием надежности в отрасли доменных имен с помощью саморегуляции и определения передовых практик, которые могут помочь интернет-пользователям идентифицировать надежные веб-сайты.⁸²

Возможные методы сбора и измерения данных

Получение обратной связи от операторов регистратур по вопросу о том, почему они решили не следовать проверке HSZ, может дать представление о причинах редкого применения этого рекомендованного механизма защиты. Кроме того, беседа с представителями fTLD Registry Services LLC о том, почему они решили применить собственную HSZ, может стать дополнительным источником данных.

Предложение и модели исследования

Возникают важные **эмпирические задачи**, касающиеся связи между расширением DNS посредством Программы New gTLD и распространением злоупотреблений и преступной деятельности в DNS. Остаются важные вопросы о том, способствовала ли Программа New gTLD росту злоупотреблений DNS, *который пропорционален увеличению размера DNS в результате Программы*, и – главное – **были ли эффективны внедренные механизмы защиты в достижении намеченных целей**. Тем не менее, данный литературный труд, сосредоточенный на злоупотреблении DNS, практически полностью состоит из исследований, строящихся на описательной статистике и прицельного рассмотрения конкретных злоупотреблений DNS, и страдает от очевидного недостатка в обобщенных продолжительных исследованиях, задействующих многофакторный, логически выведенный статистический анализ.

Для того чтобы дать исчерпывающее представление о состоянии злоупотреблений DNS в новых gTLD и оценить эффективность механизмов защиты, используемых для сведения этих злоупотреблений к минимуму, в данном отчете приводится **управляемый гипотезами** каузальный анализ, использующий механизмы защиты в качестве промежуточных переменных в наборе гипотетических моделей, построенных на обоснованных предположениях, касающихся отношений между механизмами защиты Программы New gTLD и распространением злоупотреблений DNS. Данная

⁸¹ См. fTLD Registry Services, “Enhanced Security,” по состоянию на 11 февраля 2016 года, www.ftld.com/enhanced-security/

⁸² “About the DNS Seal Project,” по состоянию на 12 февраля 2016 года, [http://dnsseal.wiki/About the DNS Seal Project](http://dnsseal.wiki/About%20the%20DNS%20Seal%20Project)

модель сосредоточена на том, чтобы ответить на главный вопрос исследования:

какая доля злоупотреблений DNS может приходиться на механизмы защиты, внедренные для сведения к минимуму злоупотреблений DNS в новых gTLD?

Для того чтобы ответ на этот вопрос был всеобъемлющим и звучал по-научному, необходимо построить проверяемую гипотетическую модель и разделить исследование на составные части, чтобы сосредоточиться на старых и/или новых TLD, и/или на всем пространстве DNS по необходимости. Для этого необходимо установить **исходный критерий** в качестве отправного пункта для ответа на фундаментальный вопрос о том, произошел ли рост злоупотреблений DNS в результате самой Программы New gTLD, т. е. был ли он *пропорционален расширению DNS*. Установив критерий, можно начать задавать **вопросы, ориентированные на коэффициенты злоупотреблений в период «до внедрения механизмов защиты» по сравнению с периодом «использования механизмов защиты» во время расширения DNS**. Это позволяет исследователям увязать с контекстом потенциальную связь между девятью механизмами защиты и текущим коэффициентом злоупотреблений DNS.⁸³

Представленные ниже модели допускают возможность применения как качественных, так и количественных методов тестирования. Однако, ссылаясь на вышесказанное, многие критерии этих механизмов защиты не выдают качественные данные, необходимые для проведения глубокого статистического анализа. Два подхода могут с этим справиться: изучение потенциальных репрезентативных данных для эффективности механизмов защиты и применение качественных методов – например, получение обратной связи от пользователей, фокус-группы, анализ подходящих публикаций – чтобы добавить эмпирическую глубину большему объему качественных методов, которые возможно применить в контексте данных механизмов защиты.

⁸³ Обратите внимание, что данный подход к сравнению коэффициента злоупотреблений в старых TLD между «периодом до Программы New gTLD» со злоупотреблением в новых gTLD был независимо использован и предпочтен разными участниками сессии на телеконференции, посвященной измерению злоупотреблений DNS и эффективности девяти механизмов защиты. См. ICANN Operations and Policy Research, “Reviewing New gTLD Program Safeguards Against DNS Abuse,” («Анализ механизмов защиты Программы New gTLD от злоупотребления DNS»), 28 января 2016 года, материалы и записи телеконференции доступны на <https://newgtlds.icann.org/en/reviews/dns-abuse>

Возможная качественная концепция для тестирования эффективности механизмов защиты

Данное предложение и указанные ниже модели представляют собой первые шаги, которые послужат основой для обсуждения самых эффективных средств тестирования эффективности механизмов защиты, внедренных для сведения к минимуму злоупотреблений DNS. CCT-RT остается определить масштабы применения и метод исследования работы, проведенной с целью сведения к минимуму злоупотреблений DNS.

План проведения исследования: Ключевые вопросы и соображения

Имеется избыток потенциальных данных — будь то в качественной или количественной форме — который потенциально можно задействовать в изучении эффективности девяти механизмов защиты, внедренных для сведения к минимуму злоупотреблений DNS. Однако, прежде чем принимать решение о том, какие данные использовать, необходимо определиться с планом проведения исследования для структурирования данных и достижения целей исследования. Любой план проведения исследования должен отвечать следующим требованиям:⁸⁴

1. Четко определите проблему исследования. Какую эмпирическую задачу мы пытаемся решить?
2. Анализ и синтез ранее опубликованной литературы, связанной с проблемой.
3. Четкая и недвусмысленная формулировка вопросов исследования и/или гипотез, имеющих центральное значение для проблемы исследования.
4. Эффективное описание данных, необходимых для корректного ответа на вопросы исследования и/или проверки гипотезы, а также объяснение способа получения таких данных.
5. Описание методов анализа, которые будут применяться к данным при определении правильности или неправильности гипотез.

Указанные ниже вопросы и ответы увязывают с контекстом эти задачи исследования в том, что касается анализа злоупотреблений DNS:

1. Четко определите проблему исследования. Какую эмпирическую задачу мы пытаемся решить?

Проблема исследования: Неясно, насколько эффективны были механизмы защиты, внедренные для сведения к минимуму злоупотреблений DNS в новых gTLD.

Эмпирическая задача: Некоторые индикаторы указывают на сокращение числа злоупотреблений DNS в TLD в целом (в старых и

⁸⁴ Взято из сжатого списка вопросов для исследования Университета Южной Калифорнии на <http://libguides.usc.edu/writingguide/researchdesigns> (по состоянию на 26 февраля 2016 года).

новых), в то время как другие указывают на увеличение коэффициентов в отдельных TLD. Остается неясным, насколько сильное влияние эти механизмы защиты, внедренные для сведения к минимуму злоупотреблений DNS, оказали на данное изменение.

2. Анализ и синтез ранее опубликованной литературы, связанной с проблемой.

Данный отчет направлен на предоставление такого анализа и синтеза.

3. Четкая и недвусмысленная формулировка вопросов исследования и/или гипотез, имеющих центральное значение для проблемы исследования.

Вопрос(ы) исследования: Чем объясняется изменение коэффициентов злоупотребления в разных TLD? Насколько эффективны были механизмы защиты, внедренные для сведения этих злоупотреблений к минимуму?

Примеры гипотез (см. предложенные ниже модели для более тщательного изучения определяющих гипотетических связей):

- Высокого уровня (служит ориентиром всего анализа или его значительной части):
 - Расширение DNS привело к *увеличению* числа злоупотреблений DNS, которое непропорционально самому расширению.
- Низкого уровня (служит ориентиром отдельных частей исследования в рамках анализа):
 - Механизм защиты X, направленный на предотвращение формы Y злоупотребления DNS, оказался неэффективным для достижения поставленных перед ним целей

В вопросах исследования и гипотезах также должно указываться определение и/или способ измерения каждого термина. Например, как указано выше, как мы измеряем «эффективность» механизма защиты?

4. Эффективное описание данных, необходимых для корректного ответа на вопросы исследования и/или проверки гипотезы, а также объяснение способа получения таких данных.

Например, «эффективность» механизмов защиты можно измерить качественно посредством проведения опросов экспертов или пользователей этих механизмов защиты. То, насколько сильно Программа New gTLD повлияла на злоупотребления DNS, вероятно, можно количественно измерить путем изучения статистических корреляций между количеством новых доменов и показателя злоупотреблений DNS, например, коэффициент фишинга.

5. Описание методов анализа, которые будут применяться к данным при определении правильности или неправильности гипотез.

Определил работа CCT-RT, помимо формулирования вопросов исследования и гипотез, как указано выше.

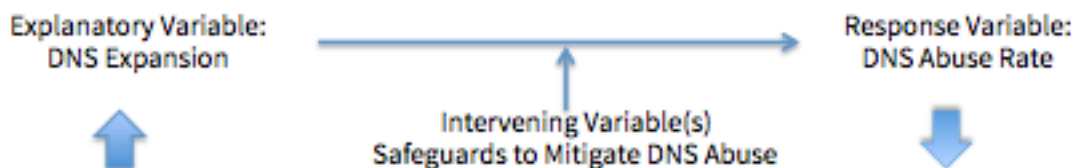
Каузальные модели и гипотезы

Приведенные ниже модели выведены из простой центральной гипотезы о том, что – по крайней мере, теоретически – введение механизмов защиты в целях предотвращения злоупотребления DNS в новых gTLD должно вести к более «чистому» (т. е. с меньшим количеством злонамеренной деятельности) пространству DNS по сравнению с периодом «старых» TLD, когда подобные механизмы защиты отсутствовали.



Из этой базовой модели выводятся три проверяемые гипотетические сценария:

Модель 1: Расширение DNS привело к пропорциональному *уменьшению* злоупотреблений DNS (Гипотеза эффективных механизмов защиты)

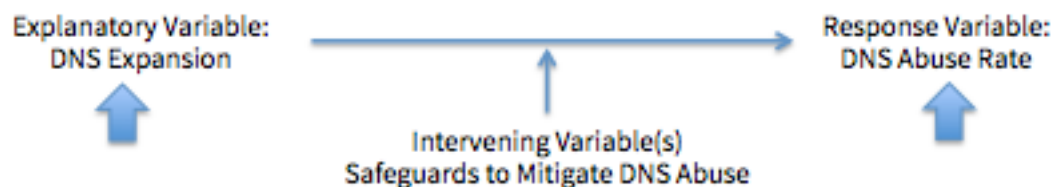


Вопрос исследования: До какой степени каузальные факторы эффективных механизмов защиты объясняют пропорциональное *уменьшение* злоупотреблений DNS?

Гипотеза 1: Расширение DNS, оснащенное механизмами защиты – это каузальный фактор, объясняющий пропорциональное **уменьшение** злоупотреблений DNS в новых и/или старых TLD, и/или во всей DNS (сегментный анализ по новым и/или старым TLD, и/или всей DNS по необходимости).

Гипотеза 1.1: Внедренные для сведения к минимуму злоупотреблений DNS механизмы защиты были **эффективны** в достижении поставленных перед ними целей и являются каузальными факторами, объясняющими пропорциональное уменьшение злоупотреблений DNS (наметить отдельные механизмы защиты для анализа по необходимости).

Модель 2: Расширение DNS посредством Программы New gTLD привело к пропорциональному **увеличению** злоупотреблений DNS (Гипотеза неэффективных механизмов защиты)

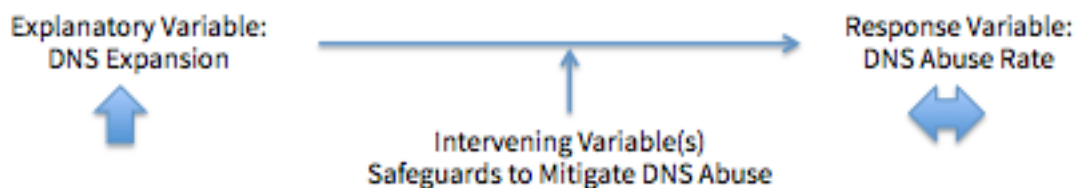


Вопрос исследования: До какой степени каузальные факторы неэффективных механизмов защиты объясняют пропорциональное **увеличение** злоупотреблений DNS?

Гипотеза 2: Расширение DNS, оснащенное механизмами защиты, – это каузальный фактор, объясняющий пропорциональное **увеличение** злоупотреблений DNS в новых и/или старых TLD, и/или во всей DNS (сегментный анализ по новым и/или старым TLD, и/или всей DNS по необходимости).

Гипотеза 2.1: Внедренные для сведения к минимуму злоупотреблений DNS механизмы защиты были **неэффективны** в достижении поставленных перед ними целей (наметить отдельные механизмы защиты для анализа по необходимости).

Модель 3: Расширение DNS не оказало *никакого* воздействия на злоупотребление DNS
(Гипотеза неэффективных механизмов защиты)



Вопрос исследования: До какой степени каузальные факторы неэффективных механизмов защиты объясняют *отсутствие изменений* в злоупотреблении DNS?

Гипотеза 3: Расширение DNS, оснащенное механизмами защиты, не оказало никакого воздействия на пропорциональную долю злоупотреблений в новых и/или старых TLD, и/или во всей DNS (сегментный анализ по новым и/или старым TLD, и/или всей DNS по необходимости).

Гипотеза 3.1: Внедренные для сведения к минимуму злоупотреблений DNS механизмы защиты были **неэффективны** в достижении поставленных перед ними целей, заключающихся в предоставлении более «безопасного» пространства новых gTLD по сравнению со старым пространством (наметить отдельные механизмы защиты для анализа по необходимости).

Ввиду того, что здесь затрагивается работа CCT-RT, данное предложение по тематике исследования представляет собой возможный подход к формированию структуры их исследования, строящейся на эффективности девяти механизмов защиты, внедренных для сведения к минимуму злоупотреблений DNS. Для подобного подхода, вероятно, потребуется нанять сторонних подрядчиков, разбирающихся в сборе и анализе статистических и качественных данных, чтобы разработать и провести настоящее исследование. CCT-RT остается определить масштабы применения и метод любого анализа. По крайней мере, данное предложение по тематике исследования может служить отправной точкой для обсуждения других возможных подходов.

Приложение: Исследование деятельности, связанной со злоупотреблением в ICANN

Проект	Сфера деятельности	Источники и ссылки
<p>Спецификация 11 Соглашения об администрировании домена верхнего уровня</p>	<p><u>Раздел 3а:</u> «Оператор регистратуры включает в Соглашение между регистратурой и регистратором требование, обязывающее регистраторов включать в свои регистрационные соглашения положение, запрещающее владельцам зарегистрированных имен распространять вредоносное программное обеспечение, принимать участие в злоупотреблениях с использованием бот-сетей, заниматься фишингом, пиратством, нарушать авторские права и права на товарные знаки, вести мошенническую или вводящую в заблуждение деятельность, распространять контрафактную продукцию и вести прочую деятельность, идущую вразрез с соответствующим законодательством. Кроме того, в этом положении должны быть указаны меры пресечения (соответствующие законодательству и любым сопряженным процедурам) такой деятельности, в том числе приостановка регистрации доменного имени».</p> <p><u>Раздел 3б:</u> «Оператор регистратуры периодически проводит технический анализ для оценки того, не используются ли домены в TLD с целью создания таких угроз безопасности, как фарминг, фишинг, распространение вредоносного ПО и эксплуатация бот-сетей. Оператор регистратуры составляет статистические отчеты о количестве обнаруженных угроз безопасности и мерах, принятых в</p>	<p>Источник: Соглашение об администрировании домена верхнего уровня</p> <p>Ссылка: Соглашения об администрировании домена верхнего уровня</p> <p>Ссылка: Часто задаваемые вопросы: Спецификация 11 Пересмотренного Соглашения об администрировании новых gTLD</p>

	результате периодических проверок безопасности. Оператор регистратуры хранит такие отчеты в течение всего срока действия Соглашения, кроме случаев, когда более короткий срок предусмотрен законом или одобрен ICANN, и предоставляет их корпорации ICANN по запросу».	
Рекомендация 11 группы по анализу SSR	<u>Рекомендация 11</u> : «ICANN должна доработать и внедрить меры по обеспечению успеха новых gTLD и ускоренного ввода IDN, которые прямо относятся к задачам программ в сфере SSR, включая средства измерения эффективности механизмов предотвращения злоупотребления системой доменных имен».	Источник: группа по анализу безопасности, стабильности и отказоустойчивости DNS Ссылка: Итоговый отчет группы по анализу безопасности, стабильности и отказоустойчивости DNS
Рекомендации GAC: ICANN53 и ICANN54	<u>Коммюнике о встрече ICANN53 в Буэнос-Айресе</u> : «GAC... рекомендует ...сообществу ICANN разработать гармонизированную методологию оценки количества неправомерно используемых доменных имен в рамках текущего выполнения оценки Программы New gTLD». <u>Коммюнике о встрече ICANN54 в Дублине</u> : «GAC рекомендует и призывает Правление ...разработать и принять гармонизированную методологию предоставления сообществу ICANN отчетов об уровнях и интенсивности злоупотреблений (например, вредоносного ПО, бот-сетей, фишинга, фарминга, пиратства, нарушения прав на товарные знаки и/или авторских прав, подделок, мошенничества, введения в заблуждение и прочих противозаконных действий), произошедших в рамках развертывания Программы New gTLD».	Источник: Правительственный консультативный комитет ICANN Ссылка: Коммюнике GAC о встрече ICANN53, Буэнос-Айрес Ссылка: Коммюнике GAC о встрече ICANN54, Дублин

<p>Консультативное заключение SSAC по вопросу защиты владельцев доменов: передовая практика сохранения безопасности и стабильности в рамках жизненного цикла управления учетными данными</p>	<p><u>Рекомендация 1:</u> «В составе периодических отчетов, отделу соблюдения договорных обязательств ICANN следует публиковать данные о заявленных регистраторами нарушениях системы безопасности в соответствии с пунктом 3.20 Соглашения об аккредитации регистраторов (RAA) 2013 года».</p> <p><u>Рекомендация 2:</u> «Положение, аналогичное пункту 3.20 RAA 2013 года, должно быть включено во все будущие договоры регистратур с публикацией статистики аналогичной той, что указана в Рекомендации 1 выше».</p>	<p>Источник: Консультативный комитет по безопасности и стабильности</p> <p>Ссылка: SAC074 Advisory</p>
<p>Индекс здоровья рынка gTLD</p>	<p>ICANN разработала ряд потенциальных положений для обсуждения сообществом, чтобы сообщить о создании Индекса здоровья рынка gTLD, который сосредоточен на (i) здоровой конкуренции, (ii) потребительском доверии и (iii) нетехнической стабильности.</p> <p>Эти предложенные положения предназначены для упрощения обсуждения сообществом того, что означает «здоровье» для глобального рынка gTLD. Ожидается, что это обсуждение сообщества принесет с собой измеряемые факторы, служащие в качестве ключевых показателей эффективности деятельности рынка gTLD.</p> <p>Ряд положений сосредоточен на злоупотреблении DNS, согласно настоящему описанию.</p>	<p>Источник: Персонал ICANN</p> <p>Ссылка: Предложение по индексу здоровья рынка gTLD: Запросы комментариев и добровольцев</p>