

Конкуренция, потребительское доверие и потребительский выбор (ССТ): новые разделы

Новые разделы, добавленные в предыдущий проект отчета

Группа по анализу конкуренции, потребительского доверия
и потребительского выбора (ССТ)
27 ноября 2017 г.



СОДЕРЖАНИЕ

1	ОСНОВНЫЕ ПОЛОЖЕНИЯ	3
1.1	Паркинг	3
1.2	Издержки владельцев брендов	4
1.3	Злоупотребление DNS	5
2	РЕКОМЕНДАЦИИ ГРУППЫ ПО АНАЛИЗУ ССТ	6
3	КОНКУРЕНЦИЯ	8
3.1	Потенциальное воздействие «паркованных» доменов на показатели конкуренции	8
3.2	Географические отличия в использовании паркинга	12
3.3	Взаимосвязь между паркингом и злоупотреблением DNS	13
3.4	Рекомендации	14
4	ПОТРЕБИТЕЛЬСКИЙ ВЫБОР	15
4.1	Предыдущие исследования	16
4.2	Выполненный группой CCTRT анализ	17
4.3	Выполненный группой CCTRT анализ: товарные знаки	18
5	МЕРЫ ЗАЩИТЫ	21
5.1	Злоупотребление DNS	21
5.1.1	Исследование злоупотребления DNS	26
5.2	Механизмы защиты прав	37
5.2.1	История создания механизмов защиты прав	37
5.2.2	Описание механизмов защиты прав	38
5.2.3	Рассмотрение этих механизмов: способствовали ли они решению проблем с защитой прав на товарные знаки и потребителей в условиях расширения пространства gTLD? 42	
5.2.4	Отчет ICANN о показателях конкуренции, потребительского доверия и потребительского выбора (ССТ)	46
5.2.5	Рекомендации	52
6	ПРИЛОЖЕНИЯ	55
6.1	Мнения меньшинства относительно документа о злоупотреблении DNS и рекомендации 4	55
6.2	Индивидуальное заявление	56
6.3	Приложение С. Опросы и исследования	58
6.4	Приложение Е. Сводные данные об участии	63

Основные положения

7 марта 2017 года группа по анализу конкуренции, потребительского доверия и потребительского выбора вынесла проект своего отчета на общественное обсуждение. В общей сложности было получено 24 комментария. В настоящее время группа их рассматривает и по мере необходимости старается учесть соответствующие соображения в окончательной версии проекта. Одновременно с периодом первоначального общественного обсуждения велась дополнительная аналитическая работа по трем направлениям: обсуждение паркинга доменов, опрос членов INTA на тему издержек владельцев брендов в связи с программой New gTLD и исследование злоупотребления DNS в пространстве новых gTLD. Каждый из этих видов аналитической деятельности привел к внесению в первоначальный проект отчета CCT изменений, которые общественность еще не имела возможности прокомментировать. Соответственно, было решено оформить дополнение к проекту отчета, чтобы предоставить такую возможность.

С учетом того, что в период первоначального общественного обсуждения уже поступило много комментариев, сейчас группа по анализу запрашивает комментарии только относительно изменений, внесенных после недавнего анализа паркинга доменов, управления брендами и злоупотребления DNS. Как указано выше, параллельно группа по анализу старается учесть комментарии, полученные во время первоначального обсуждения, и отразить их в своем итоговом отчете, который должен быть опубликован в начале января 2018 года. Пожалуйста, указывайте, к каким именно рекомендациям относятся ваши комментарии, чтобы облегчить нашу работу.

И наконец, группа по анализу хотела бы привлечь ваше внимание к рекомендации 4, которая относится к злоупотреблению DNS. Рекомендация создать процедуру под названием «Политика разрешения споров при злоупотреблении DNS (DADRP)» — это первая рекомендация CCTRT, не встретившая единодушной поддержки со стороны членов группы по анализу. Фактически, от весомого меньшинства членов группы поступило «заявление меньшинства», касающееся этой рекомендации. Был проведен опрос членов CCTRT и большинство поддержало данную рекомендацию, особенно с учетом того, что ее формулировка предусматривает необходимость обсуждения. Возможно, эта рекомендация не будет включена в состав итогового отчета, однако группа по анализу пришла к выводу, что ее стоит вынести на общественное обсуждение. Просим вас обратить особое внимание в своих комментариях на эту рекомендацию и ее обоснованность, чтобы группа по анализу смогла лучше готовность сообщества к таким мерам. Уровни злоупотребления DNS в некоторых TLD тревожно высоки, а отдел соблюдения договорных обязательств по-видимому не может или не желает выработать целостный подход к этой проблеме, решением которой могла бы стать DADARP, хотя она поднимает ряд важных моментов.

1.1 Паркинг

Учитывая высокий процент «паркованных» доменов в общем количестве регистраций в новых gTLD, даже по сравнению с относительно высоким процентом паркинга в существовавших ранее gTLD, группа по анализу постаралась понять, необходимо ли учитывать это явление при формулировании выводов о воздействии программы New gTLD на конкуренцию. Хотя было выдвинуто несколько предположений о возможном воздействии паркинга на конкуренцию, отсутствовали неопровержимые факты, позволяющие в ближайшем будущем доказать правильность таких предположений. Несмотря на то, что группа по анализу не обнаружила безусловных доказательств воздействия паркинга на конкуренцию, мы обнаружили некоторые различия среди регионов в том, что касается паркинга. В частности, по-видимому, паркованных

доменов больше среди доменных имен на китайском языке и можно предположить, что масштабы спекуляций там шире.

Возможно, есть некоторая взаимосвязь между паркингом и распространением вредоносного ПО, но это не столь существенный и однозначный показатель, как общая тенденция более низких объемов распространения вредоносного ПО, чем в существовавших ранее gTLD. Тем не менее, разница в показателях распространения вредоносного ПО между существовавшими ранее и новыми gTLD, по-видимому, сокращается, так что сообществу следует дополнительно изучить корреляцию между паркингом и распространением вредоносного ПО.

Общие результаты изучения паркинга группой по анализу не позволяют сделать окончательные выводы и говорят о необходимости дополнительного исследования, не ограниченного только новыми gTLD. Поэтому группа по анализу рекомендует собрать совокупность более точных данных о различных видах паркинга, чтобы способствовать дальнейшему изучению сообществом воздействия паркинга на конкуренцию, потребительское доверие и используемый для его оценки фактор — злоупотребление DNS.

1.2 Издержки владельцев брендов

Приступая к исследованию практического опыта, накопленного владельцами товарных знаков, Международная ассоциация по товарным знакам (INTA) провела опрос среди своих членов. Группа по анализу изучила результаты этого опроса и дополнила их результатами собственного анализа. Несмотря на относительно небольшое число респондентов, опрос INTA позволил сделать ряд интересных выводов, касающихся владельцев брендов. В результате опроса выяснилось, что «в основном регистрации в новых TLD являются дубликатами регистраций в существовавших ранее TLD или ccTLD». В частности, всего лишь 17% респондентов зарегистрировали в новых gTLD совершенно новые доменные имена, а не дубликаты тех доменов, которые уже имелись в существовавших ранее gTLD или ccTLD. Это позволяет предположить, что защитные регистрации остаются проблемой в рамках программы New gTLD. Хотя одна из заявленных целей программы New gTLD — расширение выбора для владельцев брендов, в подавляющем большинстве случаев основной причиной регистрации доменов владельцами брендов, по-видимому, является стремление защитить свои товарные знаки.

Однако результаты опроса также указывают на то, что расширение масштабов программы New gTLD сделало защитные регистрации менее эффективным средством защиты. Соответственно, денежные потоки сместились в сторону альтернативных мер защиты и расширенного мониторинга.

Более того, в результате опроса выяснилось, что в 75% случаев используются услуги сохранения конфиденциальности и регистрации через доверенных лиц, что требует дополнительного исследования.

И наконец, есть признаки того, что в новых доменах выросли издержки правоприменения, что свидетельствует о большем количестве нарушений, по сравнению с существовавшими ранее gTLD и ccTLD.

Результаты опроса INTA, как минимум, указывают на необходимость дополнительного исследования, возможно, путем проведения более простого опроса среди более широкого круга респондентов. Однако ясно, что программа New gTLD и созданные механизмы защиты прав вызвали разочарование у владельцев брендов.

1.3 Злоупотребление DNS

Группа CCTRT постаралась измерить, насколько это возможно, эффективность разработанных для программы New gTLD технических мер защиты от различных видов злоупотребления DNS. В рамках этого процесса CCTRT поручила провести всестороннее исследование злоупотребления DNS для оценки объемов злоупотреблений технического характера в существовавших ранее и новых gTLD, чтобы собрать данные для текущего анализа, которые также могли бы стать отправной точкой при выполнении анализа в будущем.

В целом, исследование злоупотребления DNS указывает на то, что создание новых gTLD не привело к увеличению общего количества злоупотреблений во всех gTLD. Тем не менее, результаты демонстрируют, что девять вышеперечисленных мер защиты сами по себе не гарантируют более низкие объемы злоупотреблений в каждом новом gTLD, по сравнению с существовавшими ранее gTLD. На самом деле, на объемы злоупотреблений скорее влияют такие факторы, как регистрационные ограничения, цена и практические методы работы конкретных регистраторов.

Результаты исследования указывают, что после создания новых gTLD сократились объемы регистрации доменов с целью рассылки спама в существовавших ранее gTLD, но при этом выросло количество злонамеренных регистраций в новых gTLD.

Группа по анализу приходит в своем отчете к выводу, что имеющиеся меры защиты не обеспечивают достаточную защиту от злоупотребления DNS и нужно изыскать творческие подходы. Мы хотели бы получить во время общественного обсуждения комментарии на эту тему.

ПРОЕКТ

2 Рекомендации группы по анализу ССТ

Рекомендации приведены в данной сводной таблице. Полный текст рекомендации вместе с соответствующими выводами и обоснованием находится в указанных главах.

- ⊙ **Предварительное условие или уровень приоритета:** согласно Уставу ICANN, группа по анализу ССТ указала, является ли выполнение каждой рекомендации обязательным условием введения в действие последующих процедур для новых gTLD. Группа по анализу решила присвоить рекомендациям, которые не были отнесены к категории предварительных условий, уровень приоритета с четко установленным сроком:
- ⊙ **Высокий приоритет:** рекомендация должна быть выполнена в течение 18 месяцев после оформления итогового отчета.
- ⊙ **Средний приоритет:** рекомендация должна быть выполнена в течение 36 месяцев после оформления итогового отчета.
- ⊙ **Низкий приоритет:** рекомендация должна быть выполнена до начала следующего анализа ССТ.

№	Рекомендация	Кому	Предварительное условие или уровень приоритета*
Глава 3. Конкуренция			
3	Собрать данные о паркинге.	Корпорации ICANN	Высокий
Глава 4. Потребительский выбор			
9	Периодически проводить опросы владельцев доменов.	Корпорации ICANN	Предварительное условие
Глава 5. Меры защиты			
A	Рассмотреть возможность поручить корпорации ICANN провести переговоры с регистратурами в рамках процедуры внесения поправок в действующие соглашения об администрировании домена верхнего уровня или при обсуждении условий новых соглашений об администрировании домена верхнего уровня во время будущих раундов создания новых gTLD, чтобы включить в эти соглашения ряд стимулов, в том числе финансовых, для принятия регистратурами, особенно с политикой открытой регистрации, активных мер по борьбе со злоупотреблениями.	Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования и РГ по PDP в отношении последующих процедур	Высокий
B	Рассмотреть возможность поручить корпорации ICANN провести переговоры с регистраторами и регистратурами в рамках процедуры внесения поправок в соглашение об аккредитации регистраторов и соглашения об администрировании	Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-	Высокий

	<p>доменов верхнего уровня для включения положений, направленных на предотвращение систематического использования конкретных регистраторов для злоупотреблений технического характера в DNS.</p>	<p>регистраторов, Организации поддержки доменов общего пользования и РГ по PDP в отношении последующих процедур</p>	
C	<p>Дополнительно изучить взаимосвязь между конкретными операторами регистратур, регистраторами и злоупотреблением DNS, заказав постоянный сбор данных, в том числе в рамках инициатив платформы отчетности о случаях злоупотребления доменами (DAAR) ICANN. Эта информация должна регулярно публиковаться для обеспечения прозрачности, позволяя выявить регистратуры и регистраторов, которых отдел соблюдения договорных обязательств ICANN в первую очередь должен подвергнуть более тщательной проверке. При обнаружении признаков злоупотребления ICANN должна составить план действий, чтобы отреагировать на результаты таких исследований, устранить выявленные проблемы и определить категории данных для постоянного сбора в будущем.</p>	<p>Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования, РГ по PDP в отношении последующих процедур и Второй группе по анализу и проверке безопасности, стабильности и отказоустойчивости DNS.</p>	<p>Высокий</p>
D	<p>Сообщество должно рассмотреть возможность разработки политики разрешения споров при злоупотреблении DNS (DADRP), распространяющей свое действие на операторов регистратур и регистраторов, у которых обнаружены чрезмерно высокие объемы злоупотреблений (например, более 10% зарегистрированных доменных имен включено в черные списки). К таким операторам регистратур или регистраторам в первую очередь нужно обратиться с требованием а) объяснить отделу соблюдения договорных обязательств ICANN причины подобного явления, б) взять обязательство в течение определенного срока устранить злоупотребления и/или принять более строгую регистрационную политику. Если ICANN не примет меры</p>	<p>Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования, РГ по PDP в отношении последующих процедур и Второй группе по анализу и проверке безопасности, стабильности и отказоустойчивости DNS.</p>	<p>Высокий</p>

	самостоятельно, можно будет применить DADRP.		
40	<p>Исследование воздействия для определения воздействия программы New gTLD на стоимость и объем усилий по защите товарных знаков в системе доменных имен, следует проводить регулярно, чтобы оценить изменение ситуации в долгосрочной перспективе, по мере развертывания программы New gTLD и увеличения количества регистраций новых gTLD. В частности, мы бы рекомендовали провести следующее исследование воздействия в течение 18 месяцев после опубликования итогового отчета CCTRT, а дальнейшие исследования проводить каждые 18–24 месяца. CCTRT признает тот факт, что это исследование было выполнено в 2017 году компанией Nielsen путем опроса членов INTA и рекомендует сохранить подобную практику, отмечая необходимость упростить участие в этих опросах.</p>	Корпорации ICANN	Высокий
41	<p>Следует провести полный анализ URS и рассмотреть аспекты ее совместимости с UDRP. Однако с учетом того, что сейчас проводится PDP для пересмотра всех RPM во всех gTLD, во время указанного анализа нужно принять во внимание отчет о результатах этого процесса разработки политики, когда тот будет опубликован, и необходимость в таком анализе может отпасть, если отчет окажется достаточно содержательным в плане выводов и всесторонней оценки потенциальных изменений.</p>	Организации поддержки доменов общего пользования	Предварительное условие
42	<p>Следует выполнить сравнительный анализ издержек и выгод, а также проверку ТМСН и круга его задач для сбора количественных данных об издержках и выгодах, связанных с текущим состоянием услуг ТМСН, что обеспечит возможность результативного пересмотра политики.</p>	Организации поддержки доменов общего пользования	Предварительное условие

3 Конкуренция

3.1 Потенциальное воздействие «паркованных» доменов на показатели конкуренции

В целом, при обсуждении воздействия новых gTLD на конкуренцию мы придерживаемся той точки зрения, что все домены равны. Однако необходимо отметить, что большинство доменов в существовавших ранее и новых gTLD не являются первичными идентификаторами типичных веб-сайтов. Вместо этого указанные домены переадресованы на другие домены (в том числе поддомены), применяются только для электронной почты, монетизируются через рекламу, или преобразование доменного имени в IP-адрес вообще не осуществляется, возможно, из-за того, что спекулянты или регистратуры держат такие домены в резерве, как домены премиум-класса. Чтобы выполнить общую оценку воздействия, группа по анализу за отсутствием более подходящего термина считала эти домены «паркованными». Группа по анализу просто попыталась определить, отличаются ли объемы этой деятельности в существовавших ранее и новых gTLD, и если да, свидетельствует ли такая разница о необходимости дополнительного исследования. Мы пришли к следующему выводу: хотя проведение дополнительного исследования было бы идеальным вариантом, возможно, его не стоит проводить в контексте программы New gTLD. Если использовать расширенное определение паркинга, согласно собранным организацией nTLDstats данным, в настоящее время около 68% доменов, зарегистрированных в новых gTLD, являются паркованными.¹ Для сравнения: на сегодняшний день в существовавших ранее gTLD количество паркованных доменов составляет 56% от общего количества регистраций. Халворсон с соавторами считают, что паркинг объясняется следующими причинами: (1) спекуляции с целью последующей продажи домена по более высокой цене; (2) отложенные планы по развитию домена; (3) неудачное развитие.²

Вот несколько вариантов поведения, которое можно считать паркингом домена:

- Не выполняется преобразование доменного имени в IP-адрес.
- Преобразование доменного имени в адрес выполняется, но попытки подключения по протоколу HTTP приводят к сообщению об ошибке.
- Подключение по HTTP выполняется успешно, но в результате отображаются рекламные объявления, предложение купить домен или и то и другое. Эти страницы могут также использоваться как средство для распространения вредоносного ПО.
- Отображаемая страница пустая или позволяет понять, что владелец домена не публикует контент.
- Отображаемая страница — это предоставленный регистратурой шаблон, в который владелец домена не внес никаких изменений.
- Домен зарегистрирован аффилированным лицом оператора регистратуры, и для него используется типовой шаблон, не содержащий уникального контента.
- С этого домена осуществляется переадресация на домен в другом TLD.

Конечно, это весьма обобщенное представление о «паркинге», так как возможности для конкуренции в каждом из описанных сценариев, скорее всего, разные. Чтобы определить воздействие на конкуренцию, во время будущего исследования потребуется индивидуально проанализировать каждую из этих категорий.

¹ «Обзор паркинга в новых gTLD» («Parking in new gTLDs Overview»), дата просмотра — 21 марта 2017 года, <https://ntldstats.com/parking/tld>

² Т. Халворсон, М. Ф. Дер, И. Фостер, С. Сэвидж, Л. К. Саул и Г. М. Фолькер, «От .academy до .zone: анализ освоения территории новых TLD» (T. Halvorson, M.F. Der, I. Foster, S. Savage, L.K. Saul, and G.M. Voelker, “From .academy to .zone: An Analysis of the New TLD Land Rush”) — материалы конференции ACM по оценке параметров интернета в 2015 году.

Тем не менее, поскольку процент «паркованных» регистраций среди новых gTLD столь велик, группа по анализу попыталась разобраться, повлияет ли этот факт на ее выводы о последствиях вывода новых gTLD на рынок и оправдает тем самым дальнейшее исследование. Можно выдвинуть различные гипотезы, предусматривающие разные алгоритмы оценки определенных видов паркованных доменов при определении рыночной доли и концентрации. Например, одна из возможных причин учитывать объемы паркинга заключается в том, что объемы продления регистраций могут отрицательно коррелировать с объемами некоторых типов паркинга, то есть текущие рыночные доли TLD с относительно высоким процентом паркованных доменов могут приводить к завышению их значимости для конкуренции в долгосрочной перспективе. Например, некоторые ранние регистрации в новых gTLD — результат «освоения новых территорий» спекулянтами. Кроме того, вначале наблюдался скачок объемов регистрации из Китая как в существовавших ранее, так и в новых gTLD, который отчасти объясняется спекуляциями, а отчасти является результатом введения нормативно-правовых положений, которые с течением времени могут измениться. Наконец, установление дифференцированных цен на первичную регистрацию и продление может оказать существенное воздействие на операции продления.³ В таком случае при оценке воздействия этих новых доменов их количество следует уменьшить на величину, соответствующую корреляции. Другими словами, если отделить спекулятивные регистрации и предположить, что вероятность их продления равна одной второй, при любых расчетах рыночной доли и концентрации количество таких доменов следует уменьшить на 50%. Конечно, необходимо учитывать возможность того, что спекулятивное поведение кардинально отличается в новых и существовавших ранее gTLD с устоявшимися рыночными ожиданиями. Согласно другой гипотезе, домены, используемые в качестве указателей, предполагают отказ от существующего домена. Другими словами, указатель может служить признаком предварительного признания нового gTLD рынком, тогда как старый домен поддерживается в краткосрочной перспективе исключительно для более плавного перехода. В этом случае количество доменов, для которых другие домены используются в качестве указателей, следует оценивать с определенным дисконтом. Конечно, в некоторых случаях переадресация означает просто «избыточную регистрацию» с целью охватить опечатки и догадки пользователей или защитить индивидуальность бренда. При дальнейшем анализе переадресации потребуется определить, какой домен используется для продвижения сайта. Наконец, есть вероятность того, что спекуляция оказывает на конкуренцию положительное воздействие, которое напрямую не определяется рыночной долей и концентрацией, помогая новичкам стать зрелыми участниками рынка, что обычно занимает 3–5 лет. Учитывая поставленную перед группой задачу изучить воздействие новых gTLD на конкуренцию, встал следующий первоочередной вопрос: сильно ли отличаются объемы паркинга в новых gTLD, по сравнению с существовавшими ранее gTLD.

Чтобы лучше разобраться в этой теме, группа по анализу воспользовалась имеющимися данными по паркингу в новых gTLD, сбором которых регулярно занимается nTLDstats. Мы также попросили ICANN заключить с nTLDstats договор для получения данных по паркингу в существовавших ранее gTLD именно для этого проекта.⁴ Мы воспользовались регистрационными данными за декабрь 2016 года, так

³ Например, во многих случаях домены XYZ изначально были бесплатными, но их продление осуществлялось по полной цене.

⁴ Компания nTLDstats применила свой алгоритм анализа паркинга к каждому из существовавших ранее gTLD, взяв за основу количество имен в файле корневой зоны. Для TLD с количеством имен 10 000 и менее nTLDstats проанализировала все зарегистрированные имена, для TLD с количеством имен 10 001–100 000 nTLDstats проанализировала 10% зарегистрированных имен, а для TLD с количеством имен более 100 000 nTLDstats проанализировала 1% зарегистрированных имен. Кроме того, nTLDstats проверила вручную 10% от общей выборки, чтобы выявить ложные результаты.

как статистические данные за этот месяц лежат в основе остальной части настоящего отчета, а также наиболее всеобъемлющим показателем паркинга, предоставленным nTLDstats, — агрегированными данными по 7 отдельным источникам паркинга.⁵

Используя эти данные, мы провели первоначальное сравнение общих объемов паркинга в существовавших ранее и новых gTLD. По оценке nTLDstats, в указанном месяце средневзвешенное количество паркованных доменов в существовавших ранее gTLD составило примерно 56%. При этом средневзвешенное количество паркованных доменов в новых gTLD за тот же месяц — около 68%, то есть почти на 20% больше, чем в существовавших ранее gTLD.⁶ Мы не знаем, какое именно воздействие оказывают паркованные домены на рыночную конкуренцию, но если такие домены в чем-то являются менее значимыми показателями конкуренции, то такая существенная разница способна повлиять на расчеты наших индикаторов конкуренции.⁷

Стараясь в общих чертах оценить потенциальную значимость показателей паркинга для будущих рыночных долей, мы попробовали определить, взаимосвязаны ли показатели паркинга и показатели продления регистрации. Чтобы провести такой анализ, мы сравнили процентные показатели паркинга в каждом TLD по состоянию на декабрь 2016 года с процентными показателями продления регистрации, рассчитанным на основе ежемесячных отчетов регистратур⁸ за период с июля по декабрь 2016 года.⁹ С помощью анализа корреляции по методу Пирсона нам не удалось выявить статистически значимую корреляцию между объемами продления регистрации и паркинга как в новых, так и в существовавших ранее gTLD. Хотя было бы интересно обнаружить такую связь, результаты этой проверки никоим образом не свидетельствуют о потенциальной корреляции. Мы рекомендуем провести более углубленные исследования данной темы, чтобы лучше понять, существует ли подобная связь. Такие исследования, помимо прочего, могут охватывать более глубокое изучение следующих факторов: 1) какие показатели паркинга позволяют лучше всего измерить рыночную конкуренцию; 2) какие показатели продления регистрации доменов следует использовать; 3) какие факторы, помимо паркинга, могут влиять на количество операций продления; 4) какова функциональная зависимость (то есть линейная, логарифмическая и так далее) между паркингом и продлением регистрации доменов; 5) насколько велико «время задержки» между паркингом и отказом от продления (то есть сколько времени проходит между паркингом домена и отказом от продления его регистрации)?

⁵ В частности, мы скорректировали объемы регистрации для каждого gTLD, чтобы отразить количество зарегистрированных доменных имен, для которых не использовался паркинг, то есть рассчитали количество регистраций для каждого gTLD (по формуле «1 минус доля паркованных доменов»). 20 процентов от 55,6 = 11,2 и 55,6 + 11,2 = 66,72 (почти 68%).

⁷ В предельном случае, если исключить все паркованные регистрации при анализе рыночной доли, выяснится, что рыночная доля «непаркованных» регистраций в новых gTLD составляет 10,9% от общего количества gTLD, то есть примерно на 23% меньше, чем доля 14,2% в случае, когда паркованные домены учитываются при вычислениях. (Аналогичная коррекция путем включения или исключения паркованных доменов при определении рыночной концентрации не привела к существенному изменению результатов.)

⁸ Регистратуры не предоставляют ICANN расчет доли операций продления регистрации. Тем не менее, с учетом автоматического продления регистрации доменов второго уровня мы вычислили процентную долю операций продления для каждого TLD, разделив количество операций продления на сумму количества операций удаления (по истечении льготного периода пробного использования доменного имени) и операций продления.

⁹ Ежемесячный процент операций продления носит довольно изменчивый характер и соответствует только той части доменов, регистрацию которых можно продлить в данном месяце, тогда как процент паркованных доменов рассчитывается, исходя из общего количества доменов в TLD. В связи с этим, для вычисления доли операций продления мы использовали шестимесячный период, чтобы при анализе минимизировать ошибки выборки.

3.2 Географические отличия в использовании паркинга

Группа по анализу также попыталась определить, меняется ли количество паркованных доменов в зависимости от региона. Например, в отчетах об исследовании рынка DNS в регионе Латинской Америки и Карибского бассейна (исследовании LAC) указано, что «по всему региону насчитывается 78% работающих и 22% неиспользуемых доменных имен gTLD (превышение времени ожидания или отсутствие активных служб)».¹⁰ Для сравнения: по данным nTLDstats, во всех новых gTLD примерно у 33% доменов нет действительных данных DNS или поступают недействительные ответы HTTP.

Хотя у группы по анализу не было возможности напрямую увязать адреса владельцев доменов с паркованными доменами, мы выявили шесть из 50 крупнейших новых gTLD, в том числе TLD, находящиеся под управлением китайских регистратур, у которых доля паркованных доменов значительно превышает их среднее количество во всех новых gTLD. При этом доля паркованных доменов варьируется от 85% у домена .wang до 98% у домена .xin. В таблице A¹¹ ниже указан процент паркованных доменов для каждого из этих шести TLD:

Доля паркованных доменов (%)	
Все новые gTLD	68%
.XIN	97,77%
.WANG	85,08%
.TOP	85,08%
网址 (xn--ses554g)	83,22%
.REN	82,82%

¹⁰ Компания Oxford Information Labs, Ассоциация доменов верхнего уровня стран Латинской Америки и Карибского бассейна (LACTLD), Европейский регистратор доменных имен в интернете (EURid) и организация InterConnect Communications, «Исследование рынка DNS в регионе Латинской Америки и Карибского бассейна» (сентябрь 2016 года), дата просмотра — 23 октября 2017 года, <https://www.icann.org/en/system/files/files/lac-dns-marketplace-study-22sep16-en.pdf>

¹¹ NTLStats.com (дата просмотра — 3 марта 2017 года): «Анализ паркинга в существовавших ранее gTLD» («Parking Analysis of Legacy gTLDs»), <https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx>

По данным nTLDstats, более 9 миллионов доменных имен в новых gTLD было зарегистрировано лицами, находящимися в Китае.¹² Одной из возможных причин более высоких объемов паркинга в тех новых gTLD, которые ориентированы на китайских владельцев доменов, является регистрация в Китае доменов для спекулятивной перепродажи, особенно коротких доменных имен (то есть содержащих не более пяти букв или цифр). В 2015 году китайские инвесторы приобрели много коротких доменных имен, так как сочли их наиболее интересным объектом инвестирования.¹³ Более того, по-видимому, китайские покупатели также приобретают доменные имена, которые подошли бы реальным конечным пользователям и, по мнению этих инвесторов, вырастут в цене. В итоге, повышение осведомленности китайских инвесторов, вкладывающих средства в доменные имена, могло способствовать более высокой доле паркованных доменов в тех новых gTLD, которые созданы в Китае. Кроме того, описанная тенденция может быть признаком спекулятивного пузыря на китайском рынке, а также ожидаемой высокой стоимости этих доменов.

Этот первичный анализ географических особенностей паркинга весьма поверхностный и выполнен на основе ограниченного объема данных, однако результаты показывают, что региональные различия в количестве паркованных доменов существуют и могут быть весьма значительными. Приведенные цифры отражают общие объемы паркинга, и при проведении анализа в будущем необходимо более детально изучить модели использования паркинга в разных географических регионах.

3.3 Взаимосвязь между паркингом и злоупотреблением DNS

Хотя группе по анализу не удалось выявить прямую связь между количеством паркованных доменов и конкуренцией или потребительским выбором, мы также рассмотрели возможность существования связи между паркованными доменами и потребительским доверием, в частности, возможность того, что паркинг ассоциируется с злоупотреблением DNS. Ранее Виссерс и соавторы¹⁴ изучили более восьми миллионов паркованных доменов и обнаружили, что «пользователи, попадающие на паркованные веб-сайты, сталкиваются с вредоносным ПО, неприемлемым контентом и изощренными видами мошенничества».¹⁵

¹² NTLStats.com (дата просмотра — 31 октября 2017 года): «Анализ паркинга в существовавших ранее gTLD» («Parking Analysis of Legacy gTLDs»), <https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx>

¹³ Эчо Хуан (Echo Huang), «Недавнее повальное увлечение китайских инвесторов короткими доменными именами» («China's newest investment craze is short domain names»), Quartz, 10 января 2016 года, дата просмотра — 30 октября 2017 года, <https://qz.com/581248/chinas-latest-investment-craze-is-short-domain-names/>

¹⁴ Виссерс, Джусен и Никифоракис «Датчики паркинга: анализ и обнаружение паркованных доменов» (Vissers, Joosen, and Nikiforakis, «Parking Sensors: Analyzing and Detecting Parked Domains») — документ, представленный на NDSS, Сан-Диего, США, 8–11 февраля 2015 года. <http://dx.doi.org/10.14722/ndss.2015.23053>

¹⁵ Группе по анализу не совсем ясно, является ли распространение вредоносного ПО умышленным действием владельцев паркованных сайтов или служб паркинга или же результатом взлома рекламных сетей. Виссерс с соавторами рассматривают такую вероятность в своем документе: «Возможно, эти сложные цепочки являются результатом процесса, сходного с арбитражем при рекламе — такая практика широко распространена среди большинства распространителей рекламы [33]. В ходе этого процесса распространитель подает заявку на доступные рекламные блоки других издателей или распространителей, разрешая перепродавать эти блоки следующему участнику торгов. Зачастую рекламные блоки перепродаются таким образом несколько раз. Как следствие, рекламные блоки уходят из-под контроля распространителя, с которым заключил партнерское соглашение первоначальный издатель. Все эти взаимодействия и посредники способны замаскировать факт прямого участия службы паркинга в распространении вредоносного ПО. Однако в некоторых случаях также осуществляется прямая доставка вредоносного ПО, например материнской компанией Parking Service 8».

При подготовке в связи с настоящей проверкой отчета «Статистический анализ злоупотреблений DNS в gTLD» выяснилось, что в целом общее количество зарегистрированных в новых gTLD доменов, связанных с вредоносным ПО, меньше, чем в существовавших ранее gTLD.¹⁶ При этом в новых gTLD процентная доля доменных имен, связанных с вредоносным ПО, по объему иногда превышает аналогичный показатель в существовавших ранее gTLD. Однако, если проанализировать долю паркованных доменов только в новых gTLD, мы увидим, что объемы распространения вредоносного ПО существенно выше в зонах с более высоким количеством паркованных доменов. Возможно, есть некоторая взаимосвязь между паркингом и вредоносным ПО, но это не столь существенный и однозначный показатель, как общая тенденция более низких объемов распространения вредоносного ПО, чем в существовавших ранее gTLD. Тем не менее, разница в показателях распространения вредоносного ПО между существовавшими ранее и новыми gTLD, по-видимому, сокращается, так что сообществу следует дополнительно изучить корреляцию между паркингом и распространением вредоносного ПО.

3.4 Рекомендации

По нашим наблюдениям, в новых gTLD процентная доля паркованных доменов (при использовании максимально широкого определения) выше, чем в существовавших ранее gTLD, а объемы паркинга доменов меняются в зависимости от региона. При этом пока неясно, оказывает ли паркинг существенное воздействие на конкуренцию или потребительский выбор. Как следствие, мы рекомендуем ICANN провести дополнительное исследование потенциального воздействия паркинга доменов на конкуренцию и воспользоваться результатами такого исследования для совершенствования анализа изменений на рынке DNS. Кроме того, мы рекомендуем ICANN использовать для этих же целей данные о предстоящих операциях удаления зарегистрированных доменов.

Рекомендация 5: Собрать данные о паркинге.

Обоснование/сопутствующие выводы: Большое количество паркованных доменов позволяет предположить, что оно оказывает воздействие на конкурентную среду, однако недостаточное количество данных делает бесплодными попытки проанализировать это воздействие.

Кому: Корпорации ICANN

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Да

Подробности: ICANN должна регулярно отслеживать долю паркованных доменов в TLD с достаточной для определения глобальных и региональных тенденций степенью детализации. Будущие проверки должны предусматривать дальнейший анализ наличия корреляции между паркованными доменами и показателями продления регистрации или других факторов, которые могут влиять на конкуренцию. Необходим дополнительный анализ связи между паркингом и злоупотреблением DNS.

Критерии успеха: Наличие важных данных, которые корпорация ICANN, подрядчики и сообщество ICANN смогут использовать при оценке конкуренции в пространстве DNS.

¹⁶ Лаборатория SIDN и Делфтский технический университет (август 2017 года), итоговый отчет «Статистический анализ злоупотреблений DNS в gTLD», дата просмотра — 23 октября 2017 года, <https://www.icann.org/en/system/files/files/sadaq-final-09aug17-en.pdf>

4 Потребительский выбор

Группа по анализу также рассмотрела вопрос о том, привело ли создание новых gTLD к расширению возможностей выбора, доступных владельцам доменов. Как было указано ранее в настоящем отчете, по мере развития программы у владельцев доменов появляются новые возможности с точки зрения выбора языков и алфавитов, географических обозначений и новых специализированных категорий. Однако мы постарались выяснить, насколько регистрация доменов в новых gTLD соответствовала действительным желаниям владельцев доменов, и не приходилось ли многим владельцам доменов регистрировать имена в новых gTLD в качестве превентивной меры для защиты своего товарного знака или личности. В частности, активно обсуждалось, в какой степени владельцы товарных знаков будут вынуждены регистрировать свои товарные знаки в качестве доменных имен в новых gTLD, чтобы этого не сделал кто-то другой.

Был выполнен ряд исследований (см. ниже) для оценки масштабов подобной «защитной» регистрации имен владельцами доменов. В преддверии этой проверки, ICANN поручила компании Nielsen провести глобальный опрос владельцев доменов, чтобы выяснить их мнение. Позже INTA провела среди своих членов опрос, результаты которого отражают практический опыт владельцев товарных знаков. Группа по анализу изучила результаты обоих исследований и дополнила их результатами собственного анализа. Вначале мы рассмотрели вопрос потребительского выбора в целом, а затем провели предметный анализ в отношении владельцев товарных знаков, как указано ниже.¹⁷

При оценке полученных результатов важно понимать, что дубликаты регистраций не всегда носят «защитный» характер. Например, владелец товарного знака может зарегистрировать один знак в нескольких доменах, чтобы повысить вероятность нахождения этого знака пользователями через поисковые системы. Эта причина становится все более весомой по мере увеличения числа доменов.¹⁸ Фактически, в общей сложности 52% опрошенных Nielsen владельцев доменов назвали в качестве одной из причин регистрации дубликатов доменных имен «чтобы обеспечить успешное обнаружение моего сайта поисковыми системами».¹⁹ Однако 51% опрошенных отметили, что прибегали к регистрации дубликатов, «чтобы защитить свой бренд или название организации», и такой же процент опрошенных указал в качестве одной из причин, «чтобы кто-то другой не смог зарегистрировать такое же имя».²⁰ В результате опроса INTA выяснилось, что «в основном регистрации в новых TLD являются дубликатами регистраций в существовавших ранее TLD или ccTLD».²¹ В частности,

¹⁷ В этой главе термин «потребители» в первую очередь обозначает владельцев доменных имен, а не конечных пользователей-потребителей, чье поведение и представления подробно описаны в главе «Доверие потребителей».

¹⁸ Следует принять во внимание пользователей, которые ищут веб-сайты, вводя интернет-адреса наугад. Увеличение количества TLD делает поиск нужного веб-сайта наугад все более сложным и среднее число попыток значительно возрастает. Учитывая этот факт, можно ожидать, что пользователи, которым неизвестен точный адрес, будут пользоваться поисковыми системами чаще, чем раньше. Однако некоторые владельцы доменов все же могут регистрировать свое доменное имя в нескольких TLD, чтобы сократить количество попыток, которые пользователю необходимо сделать при поиске веб-сайта наугад.

¹⁹ Nielsen, опрос владельцев доменов, 2-я волна (2016 год), стр. 13.

²⁰ Из того же источника. Многие владельцы доменов выбрали оба варианта ответа; в общей сложности 60% владельцев доменов в новых gTLD выбрали один из этих двух вариантов. Следует отметить, что по крайней мере некоторые респонденты указали, что зарегистрировали домены и повышения вероятности их обнаружения через поисковые системы и для защиты своего бренда или предотвращения регистрации своего имени другими лицами. Таким образом, не всегда можно отнести регистрацию исключительно к категории «защитных».

²¹ Опрос INTA, слайд 19

всего лишь 17% респондентов зарегистрировали в новых gTLD совершенно новые доменные имена, а не дубликаты тех доменов, которые уже имелись в существовавших ранее gTLD или ccTLD. Из этого следует, что «защитные» регистрации — реальное явление, причины которого, очевидно, лежат в том, что затраты на опротестование регистрации доменов другими лицами превышают затраты на регистрацию собственного товарного знака в нескольких доменах.²²

4.1 Предыдущие исследования

Изучив 1043 товарных знака компаний, входящих в список Fortune 100, Крюгер и Ван Куверинг определили следующее соотношение регистрируемых имен: (1) 100% в .com; (2) 76% в .org; (3) 84% в .net; (4) 69% в .info; (5) 65% в .biz; и (6) 57% в .mobi.²³ Зиттрейн и Эдельман обнаружили, что через 6 месяцев после начала открытой регистрации в .biz 91% выборки доменных имен в .biz был также зарегистрирован в .com, 63% были также зарегистрированы в .net, а 49% — в .org.²⁴ Компания Strategies International, проанализировав масштабы регистрации дубликатов имен и присутствие одного и того же владельца зарегистрированного имени в четырех на тот момент новых и трех существовавших ранее TLD, пришла к таким выводам: «Статистика по .info показывает, что только 11% владельцев доменов регистрировали то же самое имя в .com, из чего можно сделать вывод, что .info открыл значительные новые возможности. Если говорить о .biz, то инициатором 42% дубликатов регистраций, судя по всему, является та же самая сторона, из чего следует, что эти регистрации носят защитный характер».²⁵ Кац, Росстон и Салливан проанализировали пересечение регистрации доменов для 200 из 500 ведущих мировых брендов по рейтингу Brand Finance и обнаружили, «что значительная часть была зарегистрирована в разных TLD».²⁶ При этом, однако, они выявили «широкий диапазон среди зарегистрированных доменов с контентом» и «довольно низкий» процент активных сайтов, за исключением .com. И, наконец, Халворсон с соавторами, используя разнообразные методы поиска одинаковых владельцев доменов в зонах .com и .biz, обнаружил «как минимум некоторую степень совпадения у 40% пар [biz-com], которые удалось оценить».²⁷ Используя так называемые «явные признаки», они отнесли 11,6% доменов .biz к категории «защитных» регистраций.

²² Приложение G. Библиография содержит несколько вопросов, которые можно включить в анкеты предстоящих опросов владельцев доменных имен для лучшего понимания выбора, который они делают при регистрации доменных имен.

²³ Ф. Крюгер и Э. Ван Куверинг, «Анализ данных о регистрации товарных знаков в новых gTLD» (F. Krueger and A. Van Couvering, "An Analysis of Trademark Registration Data in New gTLDs"), рабочий документ компании Minds + Machines, (2010-02): В 51.

²⁴ Центр Беркмана по изучению интернета и общества в Гарвардской школе права, «Исследование использования домена верхнего уровня .biz» (Survey of Usage of the .biz TLD) (июнь 2002 года), дата просмотра — 25 января 2017 года, <https://cyber.law.harvard.edu/lds/001/>

²⁵ Компания Summit Strategies International, «Оценка новых gTLD: стратегические и правовые аспекты», (Evaluation of the New gTLDs: Policy and Legal Issues), июль 2004 года, дата просмотра — 25 января 2017 года, 102. Один и тот же владелец зарегистрированного имени в .com/.net/.org, стр. 102. При этом важно отметить примечание, сделанное авторами: «Данные...основаны на крайне малой выборке из 100 имен .biz и .info». Это исследование было проведено по поручению ICANN.

²⁶ М. Л. Катц, Г. Л. Росстон, Т. Салливан «Экономические аспекты расширения пространства доменов общего пользования верхнего уровня» (M.L. Katz, G.L. Rosston, and T. Sullivan, Economic Considerations in the Expansion of Generic Top-Level Domain Names), отчет о результатах этапа II: ситуационные исследования (декабрь 2011 года), дата просмотра — 25 января 2017 года, <https://archive.icann.org/en/topics/new-gtlds/phase-two-economic-considerations-03dec10-en.pdf> Были изучены домены .com, .net, .org, .biz, .info, .mobi и .us. Это исследование было проведено по поручению ICANN.

²⁷ Т. Халворсон, Дж. Журди, Г. Мэйер, М. Феледжихази, К. Крайбих, Н. Уивер, К. Левченко и В. Паксон, «Домен верхнего уровня BIZ: десять лет спустя» (T. Halvorson, J. Szurdi, G. Maier, M. Felegyhazi, S. Kreibich, N. Weaver, K. Levchenko, and V. Paxton, "The BIZ Top-Level Domain: Ten Years Later") в Passive and Active Measurement, ред. Н. Тафт (N. Taft) и Ф. Риччиато (F. Ricciato). (Германия: Springer Berlin Heidelberg, 2012 год), 221-230, 228. <http://www.icir.org/vern/papers/dot-biz.pam12.pdf>

4.2 Выполненный группой CSTRT анализ

По итогам 2-й волны глобального опроса владельцев доменов выявлено, что 35% опрошенных владельцев доменов зарегистрировали как минимум одно имя в новых gTLD.²⁸ 60% из них указали в качестве цели регистрации «защиту существующих доменов и гарантию того, что никто другой не сможет получить аналогичный домен», 34% — «привлечение новых пользователей интернета или новых групп клиентов», а 6% — «так как необходимое мне имя было недоступно в существовавших ранее gTLD».

Мы также провели анализ строк, зарегистрированных в качестве доменов второго уровня в новых gTLD, и сопоставимых строк, зарегистрированных в .com, который в настоящее время остается самым популярным из существовавших ранее gTLD. Анализ охватывал две потенциальных схемы. В первом случае мы стремились определить, была ли *идентичная строка*, зарегистрированная в качестве домена второго уровня в новом gTLD, также зарегистрирована как домен второго уровня в зоне .com (например, если было зарегистрировано доменное имя example.tld, было ли также зарегистрировано имя example.com?).²⁹ Было обнаружено, что в .com содержатся точные совпадения для 82% строк, зарегистрированных в новых gTLD. При этом наблюдалось заметное колебание процентной доли идентичных совпадений в разных gTLD. Например, из 414 gTLD с количеством регистраций не менее 1000 у 32 было как минимум 99% доменов второго уровня, полностью совпадающих с доменами в зоне .com, включая домены .wang и .xin, находившиеся на третьем и одиннадцатом месте по объемам регистрации среди новых gTLD по состоянию на ноябрь 2016 года; а почти у двух третей (271) было как минимум 95% доменов второго уровня, полностью совпадающих с доменами, зарегистрированными в зоне .com. В другом предельном случае у 10 gTLD было менее 50% доменов второго уровня, полностью совпадающих с доменами в зоне .com. Половину из них составляли IDN-домены. В целом, IDN gTLD содержали меньшее количество полных совпадений с доменными именами .com, и только 70% зарегистрированных имен в IDN gTLD полностью совпадали с доменами .com. К сожалению, так как при анализе не учитывались данные WHOIS, нам не удалось определить, были ли оба доменных имени зарегистрированы одним и тем же владельцем домена. Во втором случае мы стремились определить, была ли *комбинированная строка*, представляющая собой совокупность TLD и SLD, также зарегистрирована как домен второго уровня в зоне .com (например, если было зарегистрировано доменное имя example.tld, было ли также зарегистрировано имя example.tld.com?). В результате этого анализа выяснилось, что в зоне .com содержатся комбинированные совпадения только для 8% строк, зарегистрированных в новых gTLD.

В целом, мы пришли к следующему выводу: хотя некоторые владельцы доменов стремятся обеспечить свою защиту в новых gTLD, многие принимают решение о регистрации в новых gTLD для увеличения охвата или популярности своих товаров и услуг, даже в том случае, когда аналогичные варианты все еще доступны для регистрации в существовавших ранее gTLD.

²⁸ Nielsen, опрос владельцев доменов, 2-я волна (2016 год), стр. 164.

²⁹ Analysis Group, «Сводная информация о зарегистрированных в существовавших ранее gTLD строках товарных знаков, которые также являются TLD-брендами» («Summary of Trademark Strings Registered in Legacy gTLDs Trademark Strings that are also Brand TLDs»), октябрь 2016 года, дата просмотра — 25 января 2017 года, <https://community.icann.org/download/attachments/56135378/New%20gTLD%20Registrations%20of%20Brand%20TLD%20TM%20Strings%2010-18-16.pdf?version=1&modificationDate=1481305785167&api=v2>

4.3 Выполненный группой CSTRT анализ: товарные знаки

Проведенный INTA опрос показал, что для респондентов, владеющих товарными знаками, «основной целью регистрации почти всех новых доменов, являвшихся дубликатами имен в существовавших ранее gTLD или ccTLD, было предотвращение использования этого имени другим владельцем домена».³⁰ Чтобы лучше понять степень распространенности таких защитных регистраций среди владельцев товарных знаков, мы изучили этот вопрос вместе с Analysis Group, воспользовавшись данными о последнем раунде программы New gTLD. В частности, сначала мы выбрали ряд товарных знаков, с которыми могли быть связаны случаи защитной регистрации, и определили личности владельцев доменов. Полученные Analysis Group данные представляли собой 25% случайную выборку сведений о владельцах товарных знаков из базы данных Deloitte, которая содержит все товарные знаки, зарегистрированные в Депозитарии товарных знаков. Личности владельцев домена были установлены через базу регистрационных данных доменов WHOIS.³¹ Для анализа из Депозитария товарных знаков были отобраны только подтвержденные или исправленные строки товарных знаков, состоявшие из символов латинского алфавита. Совпадениями считались случаи точного совпадения с точки зрения критериев ICANN, если при этом владелец домена признавался владельцем товарного знака, соответствующего зарегистрированной строке, на основании приблизительного текстового сравнения имен владельца домена и владельца товарного знака.

Используя эти данные, мы определили: (1) зарегистрировал ли владелец товарного знака каждый из товарных знаков нашей выборки как минимум в одном существовавшем ранее gTLD; (2) зарегистрировал ли владелец товарного знака тот же самый товарный знак как минимум в одном новом gTLD; и (3) если строка была зарегистрирована владельцем товарного знака хотя бы в одном новом gTLD, количество новых gTLD, в которых владелец товарного знака зарегистрировал свою строку. Было обнаружено, что 54% строк, зарегистрированных в существовавших ранее gTLD, были также зарегистрированы как минимум в одном новом gTLD. Также было обнаружено, что среднее количество регистраций этих строк в новых gTLD составляет 3. Другими словами, половина проанализированных товарных знаков была зарегистрирована в 3 или менее новых gTLD.³² Кроме того, выяснилось, что три четверти этих строк зарегистрировано в 7 или менее новых gTLD, а 90% этих строк — в 17 или менее новых gTLD.³³ В то же время, небольшое количество строк товарных знаков было зарегистрировано во множестве TLD: 4% товарных знаков было зарегистрировано по крайней мере в 100 новых gTLD и один — в 406 новых gTLD. Экстраполяция выборки на все товарные знаки позволяет предположить, что на сентябрь 2016 года владельцы товарных знаков могли в совокупности выполнить 80 000 регистраций своих товарных знаков в новых gTLD, что составляет 0,3% от

³⁰ Опрос INTA, слайд 22.

³¹ Analysis Group, проект отчета о независимой проверке Депозитария товарных знаков (TMCH), июль 2016 года, дата просмотра — 25 января 2017 года, <https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf>

³² Среднее количество зарегистрированных дубликатов составило 8, но на статистику ощутимо влияет малое количество товарных знаков, зарегистрированных в очень большом количестве доменов. Например, один из товарных знаков был зарегистрирован в 406 доменах.

³³ При оценке полученных результатов важно помнить, что на наблюдаемый объем зарегистрированных дубликатов в той или иной мере повлияло использование владельцами товарных знаков услуг блокировки, описанных ранее. Другими словами, в той степени, в какой владельцы товарных знаков обеспечили защиту за счет блокировки, необходимость в защитной регистрации товарных знаков могла уменьшиться.

общего количества регистраций в новых gTLD.³⁴ На основе этого анализа можно сделать следующий вывод: хотя для большинства владельцев товарных знаков прямые расходы на защитные регистрации в связи с программой New gTLD, по-видимому, оказались ниже, чем мы опасались до запуска этой программы, небольшая часть владельцев товарных знаков, судя по всему, несет значительные расходы.

В дополнение к защитной регистрации некоторые регистратуры предлагают владельцам товарного знака услугу по блокировке использования соответствующего товарного знака другими лицами без необходимости покупки самого доменного имени. Например, Rightside предлагает «экономичное одноэтапное решение в масштабах всей регистратуры, которое обеспечивает защиту товарных знаков ваших клиентов от киберсквотинга... с помощью нашего Списка защищенных на уровне домена товарных знаков (DPML)» в качестве альтернативы «защитной покупке товарных знаков и товарных знаков+терминов в каждом TLD...»³⁵ Аналогичную услугу предлагает Donuts, сообщая, что используемый «Список защищенных на уровне домена товарных знаков (или DPML) ограждает владельцев товарных знаков от киберсквотинга за гораздо меньшую цену, чем защитная регистрация каждого термина во всех доменах Donuts»³⁶. На момент опубликования настоящего документа мы не располагали данными о расходах, которые владельцы товарных знаков несут при использовании таких услуг блокировки, но рассчитываем получить более подробную информацию до опубликования итогового отчета.

Рекомендация 9: Периодически проводить опросы владельцев доменов.

Обоснование/сопутствующие выводы: Невозможность определить мотивы и поведение владельцев доменов приводит к неудачам при изучении конкуренции и потребительского выбора на рынке TLD.

Кому: Корпорации ICANN

³⁴ В результате проверки ТМЧН с использованием 25% выборки было обнаружено 19 642 случаев регистрации владельцами своих товарных знаков. Экстраполяция этих результатов на 100% позволяет предположить, что общее количество регистраций составляет 78 568. Для сравнения, на сентябрь 2016 года во всех новых gTLD было зарегистрировано в общей сложности 24 814 734 имен.

³⁵ Регистратура Rightside, «DPML», дата просмотра — 21 сентября 2016 года, <http://rightside.co/registry/dpml/>

³⁶ Регистратура Donuts, «DPML», дата просмотра — 21 сентября 2016 года, <http://www.donuts.domains/services/dpml>. По данным domainname.com: «Три крупнейшие регистратуры доменов верхнего уровня [цитата] создали новый инструмент блокировки доменных имен. Многие заказчики предпочитают не прибегать к защитной регистрации, а такие услуги позволяют ощутимо сэкономить средства и заслуживают внимания как средство защиты важнейших брендов. Услугу предлагают три провайдера новых gTLD: Donuts (охватывающая 172 TLD) Rightside (охватывающая 36 TLD) и Minds & Machines (охватывающая 16 TLD). Инструмент блокировки позволяет владельцам товарных знаков блокировать свои знаки и связанные с ними термины на втором уровне во всех поддерживаемых новых gTLD, после однократной уплаты регистратуре необходимого сбора. Такая услуга позиционируется как экономичный метод защиты прав владельцев на товарные знаки от киберсквотинга. Блокировка позволяет владельцам товарных знаков не прибегать к защитной регистрации в TLD трех этих провайдеров. Блокировка возможна, если блокируемый термин соответствует товарному знаку, утвержденному Депозитарием товарных знаков».

«Экономичная защита доменных имен!» Domain Info, 4 ноября 2015 года, дата просмотра — 28 сентября 2016 года, <http://domainincite.com/21404-icann-retires-affirmation-of-commitments-with-us-gov>

Недавно Donuts объявила о новой версии своей услуги блокировки, которая позволит владельцам товарных знаков активировать блокировку, заплатив \$10 000. [Джек Джек Элис (Jack Jack Elis), «Donuts представила усовершенствованное средство защиты товарных знаков; эксперт выступает за внедрение более экономичных вариантов в следующем раунде gTLD», (“Donuts unveils enhanced trademark protection offering; expert urges lower cost options in next gTLD round”), World Trademark Review, 29 сентября 2016 года, дата просмотра — 29 сентября 2016 года, <http://www.worldtrademarkreview.com/blog/Detail.aspx?g=fa934d21-cfa7-459c-9b1f-f9aa61287908>

Предварительное условие или уровень приоритета: Предварительное условие

Консенсус в группе: Да

Подробности: Чтобы определить тенденции среди владельцев доменов, необходимо разработать опрос и непрерывно улучшать его структуру. Некоторые предварительные соображения касательно вопросов, которые можно задать, изложены в предыдущем проекте отчета — Приложение F. Возможные вопросы для будущего опроса потребителей.

ПРОЕКТ

5 Меры защиты

5.1 Злоупотребление DNS

Доступность доменных имен как уникальных глобальных идентификаторов сделала их проводниками инновационных технологий, в том числе тех, которые используются в злонамеренных целях. Соответственно, злоумышленники используют эти универсальные идентификаторы не по назначению в инфраструктуре киберпреступности³⁷ и направляют пользователей на веб-сайты, позволяющие совершать другие виды преступлений, такие как эксплуатация детей, нарушение прав на интеллектуальную собственность и мошенничество. Каждое из таких действий может считаться разновидностью злоупотребления DNS. Однако такие заключения во многом зависят от местного законодательства, роли других поставщиков инфраструктуры и субъективного толкования. Тем не менее, существует более твердый консенсус в отношении многих технических разновидностей злоупотребления DNS, о чем свидетельствуют результаты разработки сообществом программы New gTLD.

Из-за ненадлежащего использования доменных имен сообщество вначале высказывало опасения, что значительное увеличение количества доступных gTLD может привести к росту объемов злоупотребления DNS. Перед группой CCTRT была поставлена задача изучить вопросы, связанные с расширением DNS, в том числе реализацию мер защиты, призванных предотвратить выявленные риски.³⁸ Перед утверждением программы New gTLD ICANN обратилась к сообществу специалистов по кибербезопасности с просьбой представить мнения и предложения в отношении злоупотребления DNS и рисков, вызванных расширением пространства имен DNS.³⁹ Сообщество определило следующие области, вызывающие опасения:

³⁷ Берштейн с соавторами «Определение зависимостей, создаваемых теневой коммодитизацией», (Bursztein et al., “Framing Dependencies Introduced by Underground Commoditization”), документ, представленный в составе материалов проведенного в 2015 году семинара по экономическим аспектам информационной безопасности, Делфт, Нидерланды, 22–23 июня 2015 года), <https://research.google.com/pubs/pub43798.html>, стр. 12.

³⁸ В подписанном Министерством торговли США и ICANN документе «Подтверждение обязательств» среди вопросов, которые требовалось проанализировать перед расширением пространства доменных имен, значились «вопросы злоумышленного использования». Более того, согласно документу «Подтверждение обязательств» группа по анализу конкуренции, потребительского доверия и потребительского выбора должна проанализировать «меры защиты, реализованные ICANN для снижения последствий создания или распространения» новых gTLD. Соответственно, в мандате группы CCT сказано, что работа группы должна охватывать анализ «эффективности мер защиты» и «других усилий, направленных на противодействие злоупотреблению DNS». Кроме того, в своем коммюнике по итогам заседаний на конференции в Буэнос-Айресе в 2015 году GAC призвал сообщество ICANN «разработать гармонизированную методологию оценки количества доменных имен, используемых ненадлежащим образом, в рамках текущей оценки программы New gTLD». См. <https://gacweb.icann.org/download/attachments/27132037/BA%20MinutesFINAL.pdf?version=1&modificationDate=1437483824000&api=v2>; Аналогичным образом в коммюнике по итогам конференции в 2015 году в Дублине содержится требование к Правлению ICANN «разработать и принять гармонизированную методологию предоставления сообществу ICANN отчетов об уровнях и интенсивности недобросовестного поведения..., имевшего место в рамках развертывания программы New gTLD». См. <https://gacweb.icann.org/display/GACADV/2015-10-21+gTLD+Safeguards+%3A+Current+Round>

³⁹ «ICANN (3 октября 2009 года), *Предотвращение злонамеренного поведения*, дата просмотра — 9 ноября 2016 года, <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>. Комментарии были получены от таких групп, как Антифишинговая рабочая группа (APWG), Группа по безопасности интернет-регистратур (RISG), Консультативный комитет по безопасности и стабильности (SSAC), группы реагирования на инциденты информационной безопасности (CERT), сообщество специалистов по безопасности банковских и финансовых операций и более широкие сообщества специалистов по безопасности в интернете.

- Как нам обезопасить себя от проникновения «злоумышленников» на руководящие посты в регистратурах?
- Как нам обеспечить целостность и полезность информации о регистратуре?
- Как нам обеспечить более целенаправленную борьбу с выявленными злоупотреблениями?
- Как нам улучшить концепцию управления доменами верхнего уровня, обладающими внутренним потенциалом злонамеренного поведения?⁴⁰

Основываясь на информации, полученной от сообщества, ICANN сформулировала несколько рекомендаций в отношении мер защиты, направленных на снижение таких рисков.⁴¹ Были определены и рекомендованы девять мер защиты:

- проверка операторов регистратур;
- требование внедрить расширения безопасности системы доменных имен (DNSSEC);
- запрет на использование символов обобщения имени;
- стимулирование удаления «осиротевших» связующих записей⁴²;
- требование использовать расширенный вариант записи данных WHOIS;
- централизованный доступ к файлу корневой зоны;
- документальное оформление контактных данных и политики борьбы со злоупотреблениями на уровне регистратур и регистраторов;
- создание ускоренного процесса подачи запросов об обеспечении безопасности регистратур;
- создание проекта концепции для программы проверки зон с высокой степенью безопасности.⁴³

Группе CCTRT было поручено проанализировать эффективность девяти рекомендованных мер защиты. CCTRT в максимально возможной степени оценила эффективность каждой из этих мер защиты с использованием имеющихся данных о реализации и соблюдении требований.⁴⁴ CCTRT изучила реализацию каждой из них. Кроме того, CCTRT поручила выполнить количественный анализ злоупотребления DNS, чтобы понять возможную взаимосвязь между объемами злоупотреблений и мерами защиты, реализованными в пространстве имен новых gTLD.⁴⁵

Что касается первой из мер защиты, проверки операторов регистратур, все кандидаты на получение новых gTLD в рамках процедуры подачи и рассмотрения заявок были

⁴⁰ Из того же источника.

⁴¹ Из того же источника.

⁴² The Security Skeptic, «Осиротевшие связующие записи» («Orphaned Glue Records»), 26 октября 2009 года, дата просмотра — 2 февраля 2017 года, <http://www.securityskeptic.com/2009/10/orphaned-glue-records.html>. Это записи, которые остаются после удаления доменного имени из регистратуры.

⁴³ ICANN, «Злонамеренное поведение».

⁴⁴ См. ICANN, Меры защиты программы New gTLD (2016 год).

⁴⁵ ICANN (2 августа 2016 года), Запрос предложений в отношении исследования частотности неправильного использования DNS в новых и существовавших ранее доменах верхнего уровня, дата просмотра — 2 февраля 2017 года, <https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf>.

Исследование злоупотребления DNS содержит количественные данные о распространенных видах злоупотреблений, — в том числе об объемах спама, фишинга и распространения вредоносного ПО, — во всех gTLD с 1 января 2014 года по декабрь 2016 года. См. итоговый отчет Лаборатории SIDN и Делфтского технического университета (август 2017 года) «Статистический анализ злоупотреблений DNS в gTLD», дата просмотра — 23 октября 2017 года, <https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf>

обязаны представить полные описания внутренних технических служб, которые они предполагают использовать, даже в тех случаях, когда такие службы представлялись на условиях подряда. Такая первичная оценка должна была обеспечить техническую компетентность. Представленные описания оценивались только во время рассмотрения заявок.⁴⁶ Кроме того, все кандидаты были обязаны успешно пройти тестирование функциональности перед запуском (PDT).⁴⁷ Тестирование функциональности перед запуском включало в себя всесторонние технические испытания протокола EPP, настроек DNS-сервера, расширений безопасности системы доменных имен (DNSSEC) и прочих протоколов.⁴⁸ Делегирование доменного имени осуществлялось только после успешного прохождения кандидатами всех этих проверок.

После делегирования операторы регистратур в рамках заключаемых ими с ICANN соглашений об администрировании доменов верхнего уровня были обязаны соблюдать требования в отношении технических мер защиты. Вторая из мер защиты обязывала регистратуры gTLD внедрить DNSSEC, а также предусматривала активный контроль за соблюдением этого требования и отправку уведомлений регистратурам, не соблюдающим его.⁴⁹ DNSSEC — это набор протоколов, призванных повысить безопасность интернета за счет добавления в процесс разрешения имен DNS проверки подлинности для предотвращения таких проблем, как DNS-спуфинг⁵⁰ и отравление кэша DNS.⁵¹ Все новые gTLD используют подписание DNSSEC на уровне корневой зоны, что не означает, что все доменные имена второго уровня в этой зоне также подписываются.⁵²

Что касается третьей меры защиты, в Соглашении об администрировании домена верхнего уровня для новых gTLD запрещено использовать символы обобщения имени, чтобы гарантировать возможность разрешения доменных имен только по полному совпадению и не допустить перенаправления конечных пользователей на другие доменные имена посредством синтезированного ответа распознавателя.⁵³ Жалобы на операторов регистратур, допускающих использование символов обобщения имени, можно подавать в ICANN через онлайн-интерфейс.⁵⁴ Использование регистратурой

⁴⁶ Технические требования время от времени меняются, что затрудняет ведение непрерывного аудита.

⁴⁷ ICANN, *Руководство кандидата* (июнь 2012 года), раздел 5-4.

⁴⁸ ICANN, «Тестирование функциональности перед запуском (PDT)», дата просмотра — 2 февраля 2017 года, <https://newgtlds.icann.org/en/applicants/pdt>

⁴⁹ ICANN, «Соглашение об администрировании домена верхнего уровня», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/registries/registries-agreements-en>, Спецификация 6, статья 1.3.

⁵⁰ SANS Institute, *Глобальная сертификация целостности и безопасности информации (Global Information Assurance Certification Paper)*, дата просмотра — 2 февраля 2017 года, <https://www.giac.org/paper/qcih/364/dns-spoofing-attack/103863>. DNS-спуфинг — это ситуация, «когда DNS-сервер принимает и использует неправильные данные от узла, не имеющего полномочий на отправку таких данных» (стр. 16).

⁵¹ Суэль Сон (Soeul Son) и Виталий Шматиков, «Практическое руководство по отравлению кэша DNS» («The Hitchhiker's Guide to DNS Cache Poisoning»), документ, представленный на 6-й международной конференции ICST по безопасности и защите конфиденциальности в информационных сетях, Сингапур, 7–9 сентября 2010 года), https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. Отравление кэша DNS — ситуация, когда временно кэшированные и сохраненные распознавателем DNS данные намеренно изменяются таким образом, чтобы в процессе разрешения имен DNS выдавались IP-адреса, указывающие на недопустимые или вредоносные ресурсы (стр. 1).

⁵² ICANN, «Отчет о DNSSEC в TLD», дата просмотра — 26 апреля 2017 года, http://stats.research.icann.org/dns/tld_report/. В отчет не включены данные по домену .aero.

⁵³ ICANN, «Соглашение об администрировании домена верхнего уровня» Спецификация 6, статья 2.2

⁵⁴ ICANN, «Форма жалобы на несоблюдение запрета на символы обобщения имени (переадресацию домена)», дата просмотра — 2 февраля 2017 года, <https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form>.

символов обобщения имени легко обнаружить, поскольку в таком случае ответы даются на все запросы, вместо того, чтобы выдавать ошибку разрешения имени для недействительных доменных имен.⁵⁵ Это означает, что пользователь будет перенаправлен на похожее доменное имя. По имеющимся данным, все операторы gTLD соблюдают данную меру безопасности.⁵⁶

Для соблюдения четвертой меры защиты регистратуры новых gTLD обязаны удалять «осиротевшие» связующие записи по представлению доказательств использования таких записей для злонамеренных действий.⁵⁷ Оставленные «осиротевшие» связующие записи могут использоваться в преступных целях, например, для создания ботнетов с использованием технологии Fast Flux.⁵⁸ По своему характеру это требование не предусматривает упреждающих мер, однако операторы регистратур могут обеспечить полную техническую невозможность существования «осиротевших» связующих записей, и некоторые из них так и поступают. С 2013 года в отдел соблюдения обязательств ICANN не поступало жалоб, связанных с «осиротевшими» связующими записями.⁵⁹

Что касается пятой меры защиты, то в Соглашении об администрировании домена верхнего уровня предусмотрено требование к операторам новых gTLD создавать и поддерживать базу с расширенным вариантом записи данных WHOIS для регистрируемых доменных имен. Это означает, что помимо традиционных данных WHOIS в сокращенном варианте записи на уровне регистратуры также собирается и отображается контактная информация владельца доменного имени, а также данные контактных лиц по административным и техническим вопросам.⁶⁰ Отдел соблюдения договорных обязательств ICANN активно следит за соблюдением требования использовать расширенный вариант записи данных WHOIS как в части возможности связи с контактными лицами, так и в части формата данных.⁶¹ Правильность синтаксиса и функциональная достоверность данных оцениваются в рамках проекта ICANN по созданию системы учета достоверности данных WHOIS (ARS).⁶² В разделе «Воздействие мер защиты» настоящего отчета более подробно разъясняются вопросы, связанные с системой ARS и соблюдением соответствующих обязательств.

Кроме того, в Соглашении об администрировании домена верхнего уровня предусмотрено требование к операторам регистратур новых gTLD публиковать на своих веб-сайтах контактные данные для связи по вопросам злоупотреблений и уведомлять ICANN о любых изменениях таких контактных данных.⁶³ ICANN отслеживает соблюдение данного требования и публикует статистические данные, в том числе меры по устранению нарушений, в своих квартальных отчетах.⁶⁴

⁵⁵ <https://www.icann.org/groups/ssac/documents/sac-015-en>

⁵⁶ По состоянию на 1 января 2017 года жалоб, поданных посредством данной формы, не было. См. «Отчет о внедрении DNSSEC», дата просмотра — 1 января 2017 года, <https://rick.eng.br/dnssecstat/>

⁵⁷ ICANN, «Соглашение об администрировании домена верхнего уровня» спецификация 6, статья 4.1

⁵⁸ Консультативный комитет по безопасности и стабильности ICANN (март 2008 года), *Рекомендация SSAC в отношении хостинга Fast Flux и DNS*, дата просмотра — 2 февраля 2017 года, <https://www.icann.org/en/system/files/files/sac-025-en.pdf>

⁵⁹ ICANN, отчеты о соблюдении договорных обязательств,

<https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en>

⁶⁰ ICANN, «Что такое сокращенный и расширенный варианты записи данных WHOIS?», дата просмотра — 2 февраля 2017 года, <https://whois.icann.org/en/what-are-thick-and-thin-entries>

⁶¹ ICANN, «Соглашение об администрировании домена верхнего уровня», Спецификация 10, Раздел 4.

⁶² ICANN, «Информация о проекте создания системы учета достоверности данных WHOIS (ARS)», дата просмотра — 2 февраля 2017 года, <https://whois.icann.org/en/whoisars>

⁶³ ICANN, «Соглашение об администрировании домена верхнего уровня» Спецификация 6, раздел 4.1.

⁶⁴ ICANN, «Отчеты о соблюдении договорных обязательств за 2016 год», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en>

Соглашение об администрировании домена верхнего уровня требует от операторов регистратур реагировать на обоснованные жалобы, однако не определяет конкретные процедуры для таких действий. По этой причине не существует стандарта, позволяющего отделу соблюдения договорных обязательств ICANN оценивать конкретные меры, принимаемые операторами регистратур в рамках рассмотрения жалоб. В связи с нарушениями, касающимися контактных данных для сообщений о злоупотреблениях, было подано 55 жалоб в 2016 году,⁶⁵ 61 жалоба в 2015 году,⁶⁶ 100 жалоб в 2014 году⁶⁷ и 386 жалоб в 2013 году.⁶⁸

Что касается шестой меры защиты, в соответствии с Соглашением об администрировании доменов верхнего уровня операторы новых gTLD обязаны предоставлять файлы соответствующих зон уполномоченным отправителям таких запросов через Централизованную службу файлов корневой зоны.⁶⁹ Централизация этих источников данных расширяет возможности научных работников, занимающихся вопросами безопасности, юристов, специализирующихся на защите интеллектуальной собственности, сотрудников правоохранительных органов и других лиц, имеющих право подавать запросы и получать доступ к данным без необходимости каждый раз вступать в договорные отношения. В связи с нарушениями, касающимися массового доступа к файлам корневой зоны, было подано 19 жалоб в 2016 году,⁷⁰ 27 жалоб в 2015 году⁷¹ и 55 жалоб в 2014 году.⁷² В отчете ICANN о соблюдении договорных обязательств за 2013 год такие данные отсутствовали.

Для повышения стабильности DNS ICANN разработала Ускоренный процесс подачи запросов об обеспечении безопасности регистратур (ERSR), который позволяет регистратурам «подавать запросы для получения разрешения на отступление от требования договора в связи с действиями, которые они могут предпринять или уже предприняли, чтобы смягчить или устранить последствия» текущего или возможного в ближайшем будущем инцидента в системе безопасности.⁷³ По состоянию на 5 октября 2016 года ICANN сообщает, что процесс ERSR ни разу не использовался для новых gTLD.⁷⁴

Помимо упомянутых выше мер защиты ICANN, в ответ на комментарии сообщества, предложила создать программу проверки зон с высокой степенью безопасности, в рамках которой операторы регистратур gTLD могли бы добровольно создавать зоны с высокой степенью безопасности.⁷⁵ Консультативная группа провела обширное

⁶⁵ <https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf>

⁶⁶ ICANN, «Отчеты о соблюдении договорных обязательств за 2015 год», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/compliance-reports-2015-04-15-en>

⁶⁷ ICANN, «Отчеты о соблюдении договорных обязательств за 2014 год», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/compliance-reports-2014-2015-01-30-en>

⁶⁸ ICANN, «Отчеты о соблюдении договорных обязательств за 2013 год», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/reports-2013-02-06-en>

⁶⁹ ICANN, «Соглашение об администрировании домена верхнего уровня», Спецификация 4, раздел 2.1; ICANN, «Централизованная служба файлов корневой зоны», дата просмотра — 2 февраля 2017 года, <https://czds.icann.org/en>

⁷⁰ ICANN, «Отчеты о соблюдении договорных обязательств за 2016 год».

⁷¹ ICANN, «Отчеты о соблюдении договорных обязательств за 2015 год».

⁷² ICANN, «Отчеты о соблюдении договорных обязательств за 2014 год».

⁷³ ICANN, «Ускоренный процесс подачи запросов об обеспечении безопасности регистратур», дата просмотра — 2 февраля 2017 года, <https://www.icann.org/resources/pages/ersr-2012-02-25-en>.

⁷⁴ Отдел оказания услуг регистратурам ICANN, обсуждение по электронной почте с группой по анализу, июль 2017 года.

⁷⁵ ICANN (18 ноября 2009 года), «Модель программы проверки зон с высокой степенью безопасности», дата просмотра — 2 февраля 2017 года, <https://archive.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf>; [icann.org](https://www.icann.org), «Общественное обсуждение: Итоговый отчет о доменах верхнего

исследование, чтобы определить нормы, которые должны были бы соблюдать регистратуры для получения статуса зоны с высокой степенью безопасности. Однако из-за отсутствия консенсуса эти предложения так и не достигли этапа реализации.

Технические меры защиты, которые должны быть приняты для соблюдения договорных обязательств, подразумевают требования к регистратурам и регистраторам новых gTLD, обеспечивающие снижение рисков в связи с расширением DNS. В выполненном по поручению группы CCTRT исследовании злоупотребления DNS⁷⁶ содержится ценная информация о том, привела ли реализация этих мер защиты в целом к сокращению злоупотребления DNS по сравнению с существовавшими ранее gTLD.

5.1.1 Исследование злоупотребления DNS

В процессе подготовки к анализу группой CCTRT «мер защиты, принятых ICANN для смягчения проблем, возникших при... расширении» пространства gTLD ICANN выпустила отчет, в котором анализируется история мер по защите от злоупотребления DNS в связи с программой New gTLD.⁷⁷ При этом в отчете рассматриваются различные варианты определения понятия «злоупотребление DNS». Некоторые проблемы с определением злоупотребления DNS возникают из-за того, что в разных юрисдикциях используются разные определения и разное отношение к злоупотреблению DNS. Определенные действия считаются злоупотреблением в одной юрисдикции, но не считаются таковым в других. В зависимости от конкретной юрисдикции некоторые из этих действий, к примеру, касающиеся исключительно нарушений прав на интеллектуальную собственность, могут трактоваться по-разному не только в том, что касается их сути, но также и отношении возможных мер правовой защиты. Еще одной проблемой является недостаточное количество данных о некоторых видах злоупотреблений. Тем не менее есть типовые виды технических злоупотреблений, в отношении которых существует как консенсус, так и значительный объем данных. К ним относятся рассылка спама, фишинг, распространение вредоносного ПО и создание управляющих серверов ботнета.

В отчете ICANN признается факт отсутствия всестороннего исследования злоупотребления DNS в новых gTLD в сравнении с существовавшими ранее gTLD. Тем не менее, на основании некоторых показателей можно сделать вывод, что случаи злоупотребления DNS могут наблюдаться в значительной доле новых gTLD. К примеру, организация Spamhaus неоднократно включала новые gTLD в свой список «10 доменов верхнего уровня с наибольшим количеством злоупотреблений». Этот список составляется, исходя из доли доменных имен, имеющих отношение к злоупотреблениям, в общем количестве доменных имен в той или иной зоне.⁷⁸ Однако при этом нужно учитывать, что в ходе предыдущих исследований, проведенных компанией Architelos и Антифишинговой рабочей группой с использованием другой методологии, наибольшее количество доменных имен, имеющих отношение к

уровня с высокой степенью безопасности», 11 марта 2011 года, <https://www.icann.org/news/announcement-2011-03-11-en>

⁷⁶ ICANN, *Запрос предложенный*. Лаборатория SIDN и Делфтский технический университет, отчет «Статистический анализ злоупотреблений DNS в gTLD».

⁷⁷ ICANN, *Меры защиты программы New gTLD* (2016 год)

⁷⁸ Spamhaus, «Домены верхнего уровня, на которые приходится больше всего злоупотреблений в мире» («The World's Most Abused TLDs»), дата просмотра — 2 февраля 2017 года, <https://www.spamhaus.org/statistics/tlds/>

злоупотреблениям, было отмечено в домене .com.⁷⁹ Отчет компании PhishLabs за 2017 год также содержал вывод о том, что половина всех фишинговых сайтов находится в зоне .com, а на новые gTLD приходится всего лишь 2% всех фишинговых сайтов.⁸⁰ Однако в том же отчете отмечается, что общее количество сайтов, используемых для фишинга, в зонах новых gTLD выросло на 1000% по сравнению с предыдущим годом. По-видимому, этот вывод соответствует существенному увеличению общего количества фишинговых атак в течение 2016 года.⁸¹

Доменные имена зачастую становятся ключевым компонентом киберпреступности и позволяют злоумышленникам оперативно адаптировать свою инфраструктуру.⁸² К примеру, кампании по рассылке спама часто коррелируют с фишингом и другими видами киберпреступности.⁸³ Доменные имена также используются как вспомогательное средство при распространении вредоносного ПО и создании управляющих серверов ботнета. Статистика нарушений и происшествий, которую собирают сетевые операторы, создает впечатление, что многие новые gTLD используются исключительно для злоупотреблений.⁸⁴ Фактически, некоторые компании, работающие в сфере интернет-безопасности, рекомендовали своим клиентам заблокировать весь сетевой трафик конкретных TLD.⁸⁵ Такая практика противоречит усилиям ICANN по обеспечению универсального принятия. Между тем, помимо мер защиты, регистратуры и регистраторы предпринимают самые разные

⁷⁹ Антифишинговая рабочая группа (29 апреля 2015 года), *Отчет о тенденциях в области фишинга: 4-й квартал 2014 года*, дата просмотра — 2 февраля 2017 года, http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf; Architelos (июнь 2015 года), «Отчет NameSentrySM о злоупотреблениях за 2015 год: положение дел со злоупотреблениями в новых gTLD», дата просмотра — 2 февраля 2017 года, <http://domainnamewire.com/wp-content/Architelos-StateOfAbuseReport2015.pdf>

⁸⁰ PhishLabs, «Отчет о тенденциях в области фишинга и информационно-аналитические данные за 2017 год», стр. 23–24, <https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf>. В этот период новые gTLD занимали 8% всего рынка TLD, если исключить из массива данных домен .tk. См. Кевин Мерфи (Kevin Murphy), «Объемы фишинга в новых gTLD выросли на 1000%, однако по-прежнему хуже всего ситуация в домене .com» («Phishing in new gTLDs up 1,000% but .com still the worst»), Domain Incite, 20 февраля 2017 года, <http://domainincite.com/21552-phishing-in-new-gtlds-up-1000-but-com-still-the-worst>

⁸¹ Линдси Хейвенс (Lindsey Havens), «Выполненное APWG и Лабораторией Касперского исследование подтверждает выводы отчета о тенденциях в области фишинга и информационно-аналитические данные» («APWG & Kaspersky Research Confirms Phishing Trends & Intelligence Report Findings»), 2 марта 2017 года, опубликовано по адресу <https://info.phishlabs.com/blog/apwg-kaspersky-research-confirms-phishing-trends-investigations-report-findings>; Дарья Гудкова с соавторами, «Спам и фишинг в 2016 году», Бюллетень Лаборатории Касперского по безопасности, 20 февраля 2017 года, опубликовано по адресу <https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/>; APWG, «Отчет о тенденциях в области фишинга» («Phishing Trends Activity Report»), 23 февраля 2017 года, опубликовано по адресу http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

⁸² Symantec (апрель 2015 года), «Отчет об угрозах интернет-безопасности», дата просмотра — 2 февраля 2017 года, https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf

⁸³ Ричард Клейтон, Тайлер Мур и Генри Стерн, «Временные корреляции между веб-сайтами, используемыми для спама и фишинга» (Richard Clayton, Tyler Moore, and Henry Stern, “Temporal Correlations between Spam and Phishing Websites”), документ, представленный в материалах LEET’09 2-й конференции USENIX по вопросам крупномасштабных взломов и новых угроз, Бостон, Массачусетс, 21 апреля 2009 года, <https://www.cl.cam.ac.uk/~rnc1/leet09.pdf>

⁸⁴ Том Хендерсон, «Новые домены интернета — бросовые территории» (Tom Henderson, «The new internet domains are a wasteland»), Network World, 5 июля 2016 года, <http://www.networkworld.com/article/3091754/security/the-new-internet-domains-are-a-wasteland.html>

⁸⁵ В отчете за 2015 год компания Blue Coat рекомендовала сетевым операторам заблокировать весь входящий и исходящий трафик доменов «.work, .gg, .science, .kim и .country». См. Blue Coat, «ЗАПРЕТНАЯ ЗОНА. Исследование Blue Coat выявляет самые темные области всемирной паутины» («DO NOT ENTER Blue Coat Research Maps the Web’s Shadiest Neighborhoods»), сентябрь 2015 года, стр. 7, опубликовано по адресу <https://www.bluecoat.com/documents/download/895c5d97-b024-409f-b678-d8faa38646ab>

усилия по борьбе с ненадлежащим использованием доменных имен. Некоторые организации бездействуют до получения жалобы. Другие регистраторы, наоборот, предпринимают активные действия для анализа учетных данных владельцев доменов, блокирования строк доменных имен, похожих на известные фишинговые цели, и тщательной проверки реселлеров доменных имен, не связанных договорными обязательствами с ICANN.⁸⁶

В свете динамичного развития среды DNS, статистические данные о злоупотреблениях в gTLD не учитывают все многообразие правил регистрации и мер безопасности в сотнях новых gTLD, делегированных за период с 2013 года. Соответственно, сложно четко определить разницу в объемах злоупотреблений между существовавшими ранее и новыми gTLD без проведения всесторонней оценки. Группа CCTRT постаралась измерить, насколько это возможно, эффективность разработанных для программы New gTLD технических мер защиты от различных видов злоупотребления DNS. В рамках этого процесса CCTRT поручила провести всестороннее исследование злоупотребления DNS для оценки объемов злоупотреблений технического характера⁸⁷ в существовавших ранее и новых gTLD, чтобы способствовать получению данных для текущей проверки, которые могли бы стать отправной точкой для будущего анализа.⁸⁸ Выбранный ICANN поставщик, объединенная группа ученых Делфтского технического университета в Нидерландах (ТУ в Делфте) и специалистов Фонда регистрации доменов интернета в Нидерландах (SIDN), представила свой итоговый отчет 9 августа 2017 года.⁸⁹

Методология исследования злоупотребления DNS

Исследование злоупотребления DNS осуществлялось на основе данных файлов зон, регистрационных записей Whois и 11 отдельных источников черных списков доменных имен при вычислении объемов злоупотреблений технического характера в DNS за период с 1 января 2014 года⁹⁰ по 31 декабря 2016 года включительно.

Этот анализ охватывает следующие данные:

1. Абсолютное количество доменов, причастных к злоупотреблениям, в разрезе gTLD и регистраторов за период с 1 января 2014 года по 31 декабря 2016 года, с учетом периодов ранней регистрации и сроков предоставления всеобщего доступа к регистрации
2. Объемы злоупотреблений, которые определены из расчета «количество доменов, причастных к злоупотреблениям, на каждые 10 000» (как коэффициент нормализации, позволяющий учесть различный размер TLD), в разрезе gTLD и регистраторов за период с 1 января 2014 года по 31 декабря 2016 года
3. Злоупотребления, связанные с услугами сохранения конфиденциальности и регистрации через доверенных лиц

⁸⁶ Secure Domain Foundation, «Цена бездействия» («The Cost of Doing Nothing»), июнь 2015 года, стр. 8, https://securedomain.org/Documents/SDF_Report1_June_2015.pdf; регистраторы должны зафиксировать требования договора на более низком уровне — в составе своих соглашений с реселлерами. Однако ICANN не занимается аккредитацией реселлеров. См. Соглашение об аккредитации регистраторов, пункт 3.12 «Обязанности, связанные с предоставлением услуг регистратора третьими сторонами»

⁸⁷ Фишинг, размещение вредоносного ПО и спам. Первоначально исследовательская группа собиралась охватить при анализе домены, используемые для ботнетов. Однако, отдельные архивные данные по ботнетам в период проведения анализа не были доступны. Тем не менее, доменные имена, связанные с ботнетами (хостинг и управляющие сервера) были включены в черные списки распространителей вредоносного ПО.

⁸⁸ ICANN, Запрос предложений.

⁸⁹ Лаборатория SIDN и Делфтский технический университет, отчет «Статистический анализ злоупотреблений DNS в gTLD».

⁹⁰ Первые операции делегирования новых gTLD начались в октябре 2013 года.

4. Географическое распределение злонамеренной деятельности
5. Объемы злоупотреблений разделены по категориям «зарегистрированные со злым умыслом» и «взломанные» домены
6. Дедуктивный статистический анализ воздействия индикаторов безопасности и структурных свойств новых gTLD, (то есть количества доменов с подписью DNSSEC, паркованных доменов, количества доменов в каждом новом gTLD, а также количества доменов с контентом)

Выводы по результатам исследования злоупотребления DNS

В отчете сделано много существенных выводов относительно объемов злоупотребления DNS в новых gTLD по сравнению с существовавшими ранее gTLD. В целом, исследование злоупотребления DNS указывает на то, что создание новых gTLD не привело к увеличению общего количества злоупотреблений во всех gTLD. Тем не менее, результаты демонстрируют, что девять вышеперечисленных мер защиты сами по себе не гарантируют более низкие объемы злоупотреблений в каждом новом gTLD, по сравнению с существовавшими ранее gTLD. На самом деле, на объемы злоупотреблений скорее влияют такие факторы, как регистрационные ограничения, цена и практические методы работы конкретных регистраторов.⁹¹

Наблюдается перемещение злоупотреблений в новые gTLD

В существовавших ранее gTLD все еще зарегистрирована основная часть доменных имен и, может быть именно по этой причине, находится наибольшее количество доменных имен, используемых для фишинга и распространения вредоносного ПО.⁹² Тем не менее, общие процентные показатели злоупотреблений в существовавших ранее и новых gTLD к концу 2016 года сравнялись. При этом наблюдаются резко выраженные тенденции для конкретных видов злоупотреблений. Например, к концу 2016 года количество зарегистрированных для рассылки спама доменов в существовавших ранее gTLD снизилось, в то время как в новых gTLD наблюдался существенный рост числа таких доменных имен. В последнем квартале 2016 года 56,9 доменных имен из каждых 10 000 в существовавших ранее gTLD были включены в черные списки доменов, используемых для рассылки спама, в то время как тот же показатель для новых gTLD составил 526,6 доменных имен на каждые 10 000 регистраций.⁹³

Некоторые тенденции в плане объема злоупотреблений совпали. В пяти существовавших ранее gTLD с самой большой долей фишинговых доменов также был самый высокий процент доменных имен, связанных с распространением вредоносного ПО.⁹⁴ Большие процентные значения таких видов злоупотреблений, как фишинг и распространение вредоносного ПО, в существовавших ранее gTLD чаще являлись результатом взлома доменных имен, а не злонамеренной регистрации. Процент взломанных доменных имен в существовавших ранее gTLD намного выше, чем в новых gTLD.

В части распространения вредоносного ПО,⁹⁵ 5 новыми gTLD с максимальной долей доменных имен, использующихся для этого вида злоупотреблений, оказались .top, .wang, .win, .loan и .yuz. С конца 2015 года в домене верхнего уровня .top самая большая доля регистраций со злонамеренными целями среди всех существовавших

⁹¹ Стр. 24–25

⁹² Стр. 24

⁹³ Стр. 24

⁹⁴ Стр. 12

⁹⁵ На основании потока данных StopBadware

ранее и новых gTLD.⁹⁶ В каждом из перечисленных TLD цена регистрации была ниже, чем при регистрации доменного имени в зоне .com.

В исследовании злоупотребления DNS разделены доменные имена, зарегистрированные со злонамеренными целями, и доменные имена, зарегистрированные с законными целями, но впоследствии взломанные.⁹⁷ Результаты исследования указывают, что после создания новых gTLD сократились объемы регистрации доменов в существовавших ранее gTLD для рассылки спама, но при этом количество злонамеренных регистраций в новых gTLD выросло.⁹⁸ Это, наряду с тем фактом, что общее количество регистраций для рассылки спама практически не меняется,⁹⁹ позволяет предположить, что злоумышленники возможно отказываются от регистрации доменных имен в существовавших ранее gTLD, предпочитая новые gTLD. В рамках этой тенденции есть конкретные новые gTLD, которые в первую очередь используются для злонамеренных регистраций, чему способствует мягкая регистрационная политика и вялая борьба со злоупотреблениями или низкая цена. Фактически, деятельность некоторых регистраторов почти всецело ассоциируется со злонамеренными, а не законными регистрациями.

Злоупотребления не являются повсеместным явлением в новых gTLD

Хотя объемы злоупотреблений в новых gTLD растут, нет оснований утверждать, что они набирают обороты во всех новых gTLD. Напротив, в конце 2016 года степень концентрации этого явления была высока. Максимальная концентрация доменных имен, использовавшихся для фишинговых атак, наблюдалась в пяти новых gTLD (по данным APWG за последний квартал 2016 года), где находились 58,7% всех включенных в черные списки доменных имен, зарегистрированных в новых gTLD.¹⁰⁰ При этом организация Spamhaus включила в свой черный список не менее 10% всех доменных имен, зарегистрированных в 15 новых gTLD. Тем не менее, приблизительно в трети всех новых gTLD в последнем квартале 2016 года не было зарегистрировано ни одного случая злоупотреблений по данным черных списков.

Во время исследования у двух регистраторов были обнаружены огромные процентные доли злоупотреблений. Тревожным фактом является то, что более 93% регистраций в новых gTLD, проданных китайской компанией Nanjing Imperiosus Technology, были включены в черные списки SURBL. В течение большей части 2016 года доля злоупотреблений, связанных с этим регистратором, росла высокими темпами. В конечном итоге, ICANN приостановила деятельность Nanjing в январе 2017 года в связи с несоблюдением требований RAA.¹⁰¹ Однако причиной принятых мер не были постоянно высокие объемы злоупотреблений.

Большой объем злоупотреблений среди доменных имен .science и .top был зафиксирован еще у одного регистратора, Alpnames Ltd., находящегося в Гибралтаре. В исследовании отмечается, что этот регистратор использовал ценовое стимулирование, предлагая доменные имена по \$1 USD, а иногда даже бесплатно.¹⁰² Более того, Alpnames разрешал владельцам доменов сгенерировать случайным образом и зарегистрировать 2000 доменных имен в 27 новых gTLD в рамках одного

⁹⁶ Стр. 13

⁹⁷ К взломанным доменным именам отнесены доменные имена со взломанной регистрационной записью доменного имени или со взломанным веб-сайтом.

⁹⁸ Стр. 2

⁹⁹ См. «Исследование злоупотребления DNS», рис. 24, 36 и 38, где указано абсолютное количество доменов, используемых для рассылки спама, по данным различных источников.

¹⁰⁰ Стр. 11

¹⁰¹ https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf

¹⁰² Стр. 20

процесса регистрации. Алгоритмы массового создания доменных имен широко ассоциируются с киберпреступностью.¹⁰³ На момент опубликования данного отчета Alrnames остается регистратором, аккредитованным ICANN.

На объем или долю злоупотреблений в конкретном TLD могут влиять многие факторы. Что касается абсолютного объема, новые gTLD не отличаются от существовавших ранее gTLD в том отношении, что по мере увеличения размера TLD увеличивается количество доменных имен, используемых для злоупотреблений.¹⁰⁴ Тогда как результаты перекрестного анализа характеристик операторов регистратур TLD позволяют сделать вывод, что многие операторы с наибольшей долей злоупотреблений предлагали регистрировать доменные имена по низким ценам.

В результате исследования был сделан вывод, что зарегистрированные со злонамеренными целями доменные имена часто содержат строки, связанные с товарными знаками.¹⁰⁵ В частности, в состав 75 из 88 доменных имен .top, связанных со злоупотреблениями в четвертом квартале 2015 года, входило точное или содержащее грамматические ошибки слово Apple, iCloud или iPhone, что косвенно указывает на использование этих доменных имен для фишинговой кампании, направленной против тех, кто пользуется продукцией и услугами Apple, Inc.

В ходе исследования была обнаружена статистически неубедительная, но положительная корреляция между количеством паркованных доменов в зоне новых gTLD и процентной долей злоупотреблений.¹⁰⁶ Странно, но также наблюдалась слабая положительная корреляция между количеством доменных имен с подписью DNSSEC и объемом злоупотреблений в зоне новых gTLD.¹⁰⁷ Использование услуг сохранения конфиденциальности и регистрации через доверенных лиц, чтобы скрыть личность владельца домена в регистрационных данных Whois, шире распространено в существовавших ранее, чем в новых gTLD. В любом случае, при проведении исследования не выявлено никакой статистически значимой связи между использованием таких услуг и ненадлежащим использованием доменных имен. В первую очередь, в процессе исследования была обнаружена относительно сильная корреляция между ограничительной политикой регистрации и более низкими процентными значениями злоупотреблений. Тем не менее, даже среди новых gTLD с политикой открытой регистрации наблюдался сильный разброс доли злоупотреблений. Это позволяет предположить, что наряду с другими ключевыми переменными, например ценой, различия в практических подходах регистратур и регистраторов к борьбе со злоупотреблениями также могут влиять на долю злоупотреблений.

Злоупотребления DNS не носят случайный характер

Цена и регистрационные ограничения по-видимому учитываются киберпреступниками при выборе регистраторов и регистратур для злоупотребления DNS, делая дешевые доменные имена с легкой регистрацией привлекательным направлением для атак.¹⁰⁸ Тем не менее, эти же характеристики могут привлекать владельцев доменов с

¹⁰³ Адитья К. Суд, Шерали Зидалли, «Иерархические алгоритмы генерации доменов» (Aditya K. Sood, Sherali Zeadally, «A Taxonomy of Domain-Generation Algorithms»), IEEE Security & Privacy, том 14, стр. 46–53, июль-август 2016 года, doi:10.1109/MSP.2016.76

¹⁰⁴ Стр. 15

¹⁰⁵ Стр. 12

¹⁰⁶ Стр. 16

¹⁰⁷ Стр. 16

¹⁰⁸ Стр. 25

законными интересами, главная цель которых — бесплатный и открытый интернет. Соответственно, операторы регистратур и регистраторы могут быть материально заинтересованы в том, чтобы предотвращать систематическое злоупотребление DNS путем активной проверки регистраций и обнаружения неправомерных действий. Например, есть прецедент, когда ICANN корректировала структуру своих цен, чтобы устранить поведение, наносящее вред DNS, например отказавшись от автоматического возврата сбора за пробное использование домена.¹⁰⁹ Аналогичным образом, группа по анализу CCT предлагает найти стимулы, поощряющие внедрение передовой практики предотвращения в DNS злоупотреблений технического характера и укрепление дисциплинарных мер в случае преступного повторства таким злоупотреблениям. Этими рекомендациями можно воспользоваться и для сдерживания другого ненадлежащего использования доменных имен в объеме, который сообщество сочтет на основе консенсуса уместным для других видов злоупотребления DNS.

У нас вызывает озабоченность то, что значительные объемы злоупотреблений в DNS сконцентрированы в относительно небольшом количестве регистратур, регистраторов и географических регионов. В некоторых случаях ситуация с такими злоупотреблениями не улучшается уже в течение довольно долгого времени.

Рекомендации 1–5 сформулированы с учетом реального положения дел, когда предусмотренные для новых gTLD меры защиты сами по себе не предотвратили в DNS злоупотребления технического характера. В дополнение к имеющимся сегодня средствам предотвращения и смягчения последствий злоупотребления DNS, мы предлагаем новые стимулы и инструменты для борьбы со злоупотреблениями, которые будут:

- Поощрять и стимулировать активные меры борьбы со злоупотреблениями согласно рекомендации 1.
- Вводить новые меры по предотвращению в DNS злоупотреблений технического характера согласно рекомендации 2.
- Обеспечивать постоянный сбор данных и действия на их основании согласно рекомендации 3.
- Предусматривать создание дополнительного механизма, чтобы в тех случаях, когда, несмотря на рекомендации 1, 2 и 3, операторы регистратур или регистраторы не обеспечили результативного сокращения в DNS злоупотреблений технического характера. Необходимо рассмотреть возможность введения процедуры разрешения споров, позволяющей пострадавшим сторонам принять меры, описанные в рекомендации 4. (Обратите внимание, что группа по анализу не достигла консенсуса относительно этой рекомендации. См. заявление меньшинства в приложении 6.) Действительно, следует сделать больший акцент на работе отдела соблюдения договорных обязательств ICANN в тех случаях, когда возникает необходимость навести порядок. Если объемы злоупотреблений не снижаются в соответствии с обязательствами регистратуры, неспособность стороны, связанной договорными обязательствами, выполнить этот план должна считаться нарушением RAA/RA. Если предусмотреть такой уровень обязательств, то уменьшится не только потребность в DADRP, но и вероятность применения этой политики. Следствием этого станут положительные изменения для всех сторон благодаря сокращению объемов злоупотребления DNS.

¹⁰⁹ <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html>

Рекомендация А: Рассмотреть возможность поручить корпорации ICANN провести переговоры с регистратурами в рамках процедуры внесения поправок в действующие соглашения об администрировании домена верхнего уровня или при обсуждении условий новых соглашений об администрировании домена верхнего уровня во время будущих раундов создания новых gTLD, чтобы включить в эти соглашения ряд стимулов, в том числе финансовых, для внедрения регистратурами, особенно с политикой открытой регистрации, активных мер по борьбе со злоупотреблениями.¹¹⁰

Обоснование/сопутствующие выводы: Меры защиты, предусмотренные для новых gTLD, сами по себе не предотвращают в DNS злоупотребления технического характера. Количество злоупотреблений взаимосвязано с ограничениями регистрации, установленными для владельцев доменов, а также на него может влиять стоимость регистрации. Некоторые регистратуры изначально создавались со строгой регистрационной политикой и/или высокими ценами. Однако бесплатный, открытый и доступный интернет неизбежно подразумевает наличие регистратур с политикой открытой регистрации и низкими ценами, которые обязаны принять другие меры для предотвращения злоупотреблений технического характера в DNS. Регистратуры, которые не ограничивают регистрацию, могут сократить объем злоупотреблений технического характера в DNS, используя профилактические средства, например, идентифицируя злостных нарушителей, отслеживая подозрительные регистрации и активно выявляя злоупотребления, вместо того чтобы просто ждать жалоб. Следовательно, чтобы сократить в DNS объемы злоупотреблений технического характера в открытых gTLD, ICANN должна стимулировать принятие профилактических мер по борьбе со злоупотреблениями и вознаграждать операторов регистратур за реализацию таких мер.

Кому: Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования и РГ по PDP в отношении последующих процедур

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Да

Подробности: Правление ICANN должно рассмотреть возможность настоятельно рекомендовать корпорации ICANN провести переговоры с регистратурами, чтобы включить в состав соглашений об администрировании доменов верхнего уровня скидки при определении размера взносов, доступные операторам регистратур с

¹¹⁰ CCTRT проанализировала практические примеры, которые могли бы способствовать профилактике злоупотреблений. Одним из таких примеров является подход EURid, оператора регистратуры .EU, которая скоро начнет тестирование системы отложенного делегирования. См. <https://eurid.eu/en/news/eurid-set-to-launch-first-of-its-kind-domain-name-abuse-prevention-tool/> и https://eurid.eu/media/filer_public/9e/d1/9ed12346-562d-423d-a3a4-bcf89a59f9b4/eutldecosystem.pdf. Этот процесс не будет препятствовать регистрации. Вместо этого предусмотрена задержка активации зарегистрированного доменного имени, в отношении которого возникли подозрения в возможном злоупотреблении. Будущие группы по анализу могли бы изучить эту практику, чтобы оценить ее эффективность и возможность применения в качестве инновационной модели, способствующей укреплению доверия и созданию безопасной интернет-среды. Кроме того, еще одним примером профилактики злоупотреблений могла бы стать деятельность регистратуры .XYZ. Регистратура .xuz проводит политику абсолютной нетерпимости в отношении злоупотреблений в зоне .xuz и любых других расширений доменных имен, находящихся под ее управлением, используя передовое средство контроля злоупотреблений, позволяющее вести упреждающий мониторинг и выявлять нарушения практически в режиме реального времени, приостанавливая работу доменов, уличенных в любой неправомерной деятельности. Будущие группы по анализу могли бы оценить эффективность такого подхода, изучив динамику изменения количества злоупотреблений с течением времени и сравнив объем злоупотреблений до и после реализации этой политики.

политикой открытой регистрации, которые принимают профилактические меры для предотвращения в своей зоне DNS злоупотреблений технического характера.

Рекомендация Б: Рассмотреть возможность поручить корпорации ICANN провести переговоры с регистраторами и регистратурами в рамках процедуры внесения поправок в соглашение об аккредитации регистраторов и соглашения об администрировании доменов верхнего уровня для включения положений, направленных на предотвращение систематического использования конкретных регистраторов для злоупотреблений технического характера в DNS.

Обоснование/сопутствующие выводы: Действующая политика направлена на рассмотрение индивидуальных жалоб на злоупотребления. Однако регистраторы и операторы регистратур с чрезвычайно высокой долей злоупотреблений технического характера в DNS продолжают работать, и у них мало стимулов для того, чтобы заниматься предотвращением таких злоупотреблений. Более того, в настоящее время существует мало механизмов правоприменения для предотвращения систематического ненадлежащего использования доменных имен, связанного с деятельностью реселлеров. Систематическое использование конкретных регистраторов и регистратур для злоупотреблений технического характера в DNS угрожает безопасности и стабильности DNS, универсальному принятию доменов верхнего уровня и потребительскому доверию.

Кому: Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования и РГ по PDP в отношении последующих процедур

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Да

Подробности: Правление ICANN должно рассмотреть возможность поручить корпорации ICANN провести переговоры в рамках процедуры внесения поправок в соглашение об аккредитации регистраторов и соглашение об администрировании доменов верхнего уровня для включения положений, направленных на предотвращение систематического использования конкретных регистраторов для злоупотреблений технического характера в DNS. Такие формулировки должны возлагать на регистраторов и аффилированные с ними организации, например на реселлеров, обязанность ограничивать злоупотребления технического характера в DNS, позволяя ICANN приостанавливать деятельность регистраторов и операторов регистратур, у которых обнаружена не снижающийся, аномальный и чрезвычайно высокий процент злоупотреблений технического характера. ICANN должна делать соответствующие выводы на основе данных из нескольких проверенных и заслуживающих доверия источников, и такие выводы могут быть опровергнуты регистратором, который представит достаточное доказательство того, что выводы были неправильными. При вынесении решения могут учитываться следующие факторы, относящиеся к деятельности регистратора или оператора регистратуры: 1) принимает ли он профилактические меры для предотвращения злоупотреблений технического характера в DNS, 2) был ли он сам пострадавшей стороной в соответствующем случае, 3) выполнены ли после этого необходимые и целесообразные действия для прекращения злоупотребления и предотвращения систематического использования его служб для злоупотреблений технического характера в DNS.

Рекомендация В: Дополнительно изучить взаимосвязь между конкретными операторами регистратур, регистраторами и злоупотреблением DNS, заказав постоянный сбор данных, в том числе в рамках инициатив платформы отчетности о случаях злоупотребления доменами (DAAR) ICANN. Для обеспечения прозрачности эта информация должна регулярно публиковаться, позволяя выявить регистратуры и регистраторов, которых отдел соблюдения договорных обязательств ICANN в первую очередь должен подвергнуть более тщательной проверке. При обнаружении признаков злоупотребления ICANN должна составить план действий, чтобы отреагировать на результаты таких исследований, устранить выявленные проблемы и определить категории данных для постоянного сбора в будущем.

Обоснование/сопутствующие выводы: При исследовании злоупотребления DNS, выполненного по поручению CCTRT, был обнаружен чрезвычайно высокий процент злоупотреблений у конкретных регистратур и регистраторов, а также в связи с определенными функциональными возможностями регистрации, такими как массовая регистрация, которая по-видимому способствует злоупотреблениям. Более того, в результате исследования был сделан вывод о том, что регистрационные ограничения коррелируют со злоупотреблениями. Это подразумевает необходимость учитывать многие факторы при экстраполяции общих тенденций совершения злоупотреблений в TLD на конкретных операторов регистратур и регистраторов. Исследование злоупотребления DNS привлекло внимание к определенному поведению, которое диаметрально противоположно стимулированию потребительского доверия в DNS. Определенные регистратуры и регистраторы по-видимому прямо поощряют или по крайней мере умышленно игнорируют злоупотребление DNS. Такое поведение требуется быстро выявлять, а отдел соблюдения договорных обязательств ICANN обязан незамедлительно принять необходимые меры.

Кому: Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования, РГ по PDP в отношении последующих процедур и Второй группе по анализу и проверке безопасности, стабильности и отказоустойчивости DNS.

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Да

Подробности: Дополнительные исследования должны носить постоянный характер, обеспечивая сбор необходимых данных о злоупотреблении DNS как на уровне регистраторов, так и на уровне регистратур. Эти данные необходимо регулярно публиковать, тем самым позволяя сообществу и отделу соблюдения договорных обязательств ICANN, в частности, выявлять регистратуры и регистраторов, которых нужно проверить с большей тщательностью на предмет соблюдения договорных обязательств, чтобы устранить подобное поведение.

Рекомендация Г: Сообщество должно рассмотреть возможность разработки политики разрешения споров при злоупотреблении DNS (DADRP), распространяющей свое действие на операторов регистратур и регистраторов, у которых обнаружены чрезмерно высокие объемы злоупотреблений (например, более 10% зарегистрированных доменных имен включено в черные списки). К таким операторам регистратур или регистраторам в первую очередь нужно обратиться с требованием а) объяснить отделу соблюдения договорных обязательств ICANN причины подобного явления, б) взять обязательство в течение определенного срока

устранить злоупотребления и/или принять более строгую регистрационную политику. В случае невыполнения данного требования, если ICANN не примет меры самостоятельно, то будет задействована DADRP.

Обоснование/сопутствующие выводы: При исследовании злоупотребления DNS, выполненного по поручению CCTRT, был обнаружен чрезвычайно высокий процент злоупотреблений у конкретных регистратур. Важно создать механизм противодействия таким злоупотреблениям, в частности, если их объем велик в конкретных регистратурах. Необходимо устранить в DNS ненадлежащее поведение, и этот механизм стал бы дополнительным рычагом в борьбе со злоупотреблениями.

Кому: Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования, РГ по PDP в отношении последующих процедур и Второй группе по анализу и проверке безопасности, стабильности и отказоустойчивости DNS.

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Консенсус большинства, но не единое мнение (см. заявление меньшинства в [приложении 6.1 «Заявление меньшинства»](#))

Подробности: Отдел соблюдения договорных обязательств ICANN — одно из средств устранения этого высокого уровня злоупотребления DNS. Этот отдел контролирует соблюдение всех действующих положений и любых поправок к Соглашению об аккредитации регистраторов, предотвращая систематическое использование конкретных регистраторов для злоупотреблений технического характера в DNS в соответствии с рекомендацией 2. Однако помимо этого следует рассмотреть возможность введения специальной DADRP, которая тоже могла бы принести большую пользу в борьбе со злоупотреблением DNS и при этом также могла бы служить существенным сдерживающим средством и способствовать предотвращению или минимизации этих высоких уровней злоупотребления DNS. Операторы регистратур или регистраторы, у которых обнаружены чрезмерно высокие объемы злоупотреблений (например, когда у оператора регистратуры более 10% доменных имен включено в один или несколько разных черных списков (StopBadware SDP, APWG, Spamhaus, Secure Domain Foundation, SURBL и CleanMX)). DADRP должна предусматривать конкретные штрафные санкции. Примеры новых gTLD, у которых при исследовании злоупотребления DNS обнаружено более 10% доменных имен в черных списках, в частности, по данным Spamhaus: .SCIENCE (51%), .STREAM (47%), .STUDY (33%), .DOWNLOAD (20%), .CLICK (18%), .TOP (17%), .GDN (16%), .TRADE (15%), .REVIEW (13%) и .ACCOUNTANT (12%). Таким образом, каждую из этих регистратур следует обязать проверить факт использования своих доменных имен второго уровня для злоупотребления DNS и объяснить причины этого, взять на себя обязательство в течение определенного срока навести порядок и при необходимости принять более строгую регистрационную политику, обеспечив наличие соответствующих договорных положений, позволяющих эффективно устранять такие регистрации. Если вопрос с доменными именами не будет решен надлежащим образом, и если ICANN не примет срочные меры, пострадавшая сторона сможет воспользоваться политикой DADRP. Этот процесс должен предусматривать отправку регистратуре письменной жалобы, определенный срок ответа этой регистратуры и прения сторон. Окончательные решения должна принимать экспертная комиссия, которая могла бы рекомендовать один или несколько механизмов правоприменения, которые необходимо согласовать с сообществом.

Применительно к этой рекомендации, регистратор, действующий под контролем оператора регистратуры, должен быть охвачен политикой DADRP, поэтому важно обеспечить, чтобы «оператором регистратуры» считалось лицо, прямо или косвенно контролирующее, контролируемое или находящееся под общим контролем с оператором регистратуры, будь то посредством собственности или контроля над ценными бумагами с правом голоса, на основании договора или иным образом, где «контроль» означает прямое или косвенное обладание правом направлять или формировать направление деятельности или политики лица, будь то в результате собственности на ценные бумаги, контроля над ними, по контракту или иным образом.

5.2 Механизмы защиты прав

Новые механизмы защиты прав (RPM) были созданы специально для программы New gTLD в дополнение к существующим механизмам защиты прав. Группа по анализу конкуренции, потребительского доверия и потребительского выбора (ССТ) изучила вопрос о том, способствуют ли эти RPM повышению безопасности среды и укреплению потребительского доверия к системе доменных имен (DNS), а также постаралась определить воздействие программы New gTLD на расходы владельцев интеллектуальной собственности.

Прежде чем перейти к рассмотрению этих механизмов и их полезности при решении проблем, связанных с защитой прав на товарные знаки и потребителей в условиях расширения пространства gTLD, для полноты мы представили описание самих RPM. Группа по анализу ССТ столкнулась с очевидными трудностями при попытке получить достоверные данные, которые нужны для такой оценки, и в первую очередь обратилась к данным, собранным ICANN в составе отчетов о показателях ССТ,¹¹¹ и к данным выполненного INTA исследования воздействия,¹¹² а также к данным и комментариям, полученным в процессе анализа механизмов защиты прав ICANN, и в пересмотренном отчете о независимой проверке услуг Депозитария товарных знаков (ТМЧН).¹¹³

Кроме того, группа по анализу ССТ обратила внимание на параллельную деятельность рабочих групп, в настоящее время изучающих механизмы защиты прав, стремясь не мешать этой работе и не дублировать ее, и ждет возможности ознакомиться с отчетами этих групп.

5.2.1 История создания механизмов защиты прав

До расширения пространства gTLD в 2012 году основным механизмом защиты прав в DNS, помимо принятия решений судебными органами, была UDRP — процедура альтернативного разрешения споров, принятая ICANN 26 августа 1999 года и распространяющая свое действие на все домены общего пользования верхнего уровня. Однако еще до увеличения количества gTLD в 2012 году были выявлены проблемы, связанные с защитой товарных знаков. В частности, сообщество

¹¹¹ ICANN, «Отчетность по показателям конкуренции, потребительского доверия и потребительского выбора (ССТ)», дата просмотра — 10 октября 2017 года, <https://www.icann.org/resources/reviews/cct/metrics>

¹¹² Nielsen, опрос INTA для оценки воздействия новых gTLD на расходы (апрель 2017 года), дата просмотра — 14 сентября 2017 года: community.icann.org/download/attachments/56135378/INTA_Cost_Impact_Report_revised_4-13-17_v2.1.pdf

¹¹³ Analysis Group, проект отчета о независимой проверке Депозитария товарных знаков (ТМЧН), июль 2017 года, дата просмотра — 10 января 2017 года, <https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf>

владельцев товарных знаков выразило обеспокоенность по поводу того, что одного этого механизма будет недостаточно для адекватной защиты прав на товарные знаки и потребителей в расширенной DNS. Поэтому 6 марта 2009 года Правление ICANN постановило сформировать группу представителей разных стран, обладающих знаниями, навыками и опытом в области защиты товарных знаков, защиты потребителей, законодательства о конкуренции и понимающих взаимосвязь между товарными знаками и DNS, для подготовки решений по комплексному вопросу защиты товарных знаков в связи с появлением новых gTLD.¹¹⁴ Эту группу назвали Группой по подготовке рекомендаций по реализации (IRT).

IRT предложила ряд новых механизмов защиты прав, а именно: Служба быстрой приостановки (URS); Процедура разрешения разногласий после делегирования (PDDRP); Процедура разрешения разногласий в отношении товарных знаков после делегирования (TM-PDDRP); Процедура разрешения разногласий в отношении ограничений регистратур (RRDRP); Процедура разрешения споров в области обеспечения общественных интересов (PICDRP); Депозитарий товарных знаков (Служба ранней регистрации и Служба обработки претензий в отношении товарных знаков).¹¹⁵

5.2.2 Описание механизмов защиты прав

5.2.2.1 Единая политика разрешения споров о доменных именах (UDRP)

Единая политика разрешения споров о доменных именах (UDRP) — это утвержденная ICANN 26 августа 1999 года процедура альтернативного разрешения споров, действие которой распространяется на все домены общего пользования верхнего уровня (gTLD), в том числе существовавшие ранее gTLD (такие как com, .net, .info), новые gTLD и некоторые принявшие эту политику национальные домены верхнего уровня (ccTLD). Чтобы выиграть спор в рамках UDRP, истец должен продемонстрировать наличие более веских доказательств по следующим трем основным пунктам: (i) зарегистрированное ответчиком доменное имя идентично или сходно до степени смешения с товарным знаком или знаком обслуживания, правами на который обладает истец; (ii) у ответчика нет прав или законных интересов в отношении доменного имени; (iii) доменное имя зарегистрировано и используется со злым умыслом.

Процедура UDRP с момента подачи жалобы до принятия решения длится приблизительно 2 месяца. Стоимость подачи иска UDRP составляет от 1 500 долларов США за 1–5 доменных имен (комиссия в составе одного члена) до 4 000 долларов США за 1–5 доменных имен (комиссия в составе трех членов) за вычетом расходов на услуги юристов. Средства защиты, доступные в UDRP, ограничиваются передачей или отменой регистрации доменного имени. Материальная компенсация и механизм апелляции не предусмотрены. В большинстве случаев решение приводится в

¹¹⁴ ICANN, «Резолюции, принятые Правлением: Мексика. Защита товарных знаков в новых gTLD», 6 марта 2009 года, <https://www.icann.org/resources/board-material/resolutions-2009-03-06-en#07>.

¹¹⁵ Кроме того, для заявок на сами gTLD были введены процедуры урегулирования споров в связи со схожестью строк, ограничением общественных интересов, возражением сообщества и возражением на основании факта нарушения законных прав. Эти процессы подробнее рассмотрены в разделе «Заявка и оценка».

исполнение по прошествии 10 рабочих дней после уведомления о решении, если не было начато рассмотрение дела в суде компетентной юрисдикции.

Иски в рамках UDRP подаются в электронной форме через одобренного ICANN поставщика услуг по разрешению споров. На данный момент ICANN одобрены следующие поставщики услуг: Азиатский центр разрешения разногласий в отношении доменных имен (ADNDRC), Национальный арбитражный форум (NAF), Всемирная организация по охране интеллектуальной собственности (ВОИС), Арбитражный центр по разногласиям в интернете Чешского арбитражного суда (CAC) и Арабский центр разрешения разногласий в отношении доменных имен (ACDR).

5.2.2.2 Служба быстрой приостановки (URS)

Служба быстрой приостановки (URS) — это запущенная в 2013 году процедура альтернативного разрешения споров, изначально предназначенная для очевидных случаев киберсквоттинга в пространстве новых доменов общего пользования верхнего уровня (gTLD); однако она была добровольно принята несколькими ccTLD и «спонсируемыми» TLD, такими как .pw, .travel, .pro и .cat. Основные требования URS сходны с таковыми для UDRP, хотя требования к бремени доказывания в данном случае более жесткие («четкое и убедительное свидетельство», а не «наличие более веских доказательств»). Истец должен представить доказательства по следующим трем основным пунктам: (1) доменное имя идентично или сходно до степени смешения со словесным товарным знаком: (а) зарегистрированным на имя истца на национальном или региональном уровне и используемым в настоящее время, (б) проверенным в ходе судебного разбирательства, (в) прямо защищенным законом или международным договором, имевшим силу на момент подачи иска через URS (раздел 1.2.6.1 URS); (2) у владельца домена нет прав или законных интересов в отношении доменного имени (раздел 1.2.6.2 URS); (3) доменное имя зарегистрировано и используется со злым умыслом (1.2.6.3 URS). Объем иска не должен превышать 500 слов. URS предназначена для наиболее очевидных случаев киберсквоттинга и, как правило, не подходит для разногласий в отношении доменных имен, затрагивающих более сложные, действительно спорные вопросы (такие как добросовестность использования).

Единственное средство защиты, доступное в URS, — это приостановка действия доменного имени, а не его передача или аннулирование регистрации (средства, доступные в UDRP).

Согласно правилам URS действие доменного имени может быть приостановлено быстро — через три недели с момента подачи иска. В случае принятия решения в пользу истца действие доменного имени приостанавливается до истечения срока его регистрации (который может быть продлен еще на год). На веб-сайте, связанном со спорным доменным именем, публикуется объявление «Работа этого сайта приостановлена», но в записи WHOIS доменного имени по-прежнему будут отображаться данные первоначального владельца домена (за исключением переадресации DNS-серверов). Если решение принято в пользу истца заочно, владелец домена может потребовать повторного рассмотрения дела, направив ответ в течение шести месяцев после уведомления о заочном решении (по просьбе владельца домена этот период может быть продлен еще на шесть месяцев). На случай отказа выполнить решение в URS предусмотрен механизм апелляции на основании имеющихся документов.

Стоимость подачи иска через URS составляет около 375 долларов США (за 1–14 доменных имен).

Пока аккредитованы только три поставщика услуг URS: Азиатский центр разрешения разногласий в отношении доменных имен (ADNDRC), Национальный арбитражный форум (NAF) и компания MSFD Srl (находится в Милане, Италия).

5.2.2.3 Процедуры разрешения разногласий после делегирования (PDDRP)

5.2.2.4 Процедуры разрешения разногласий после делегирования — это механизмы защиты прав, предназначенные для защиты от действий оператора регистратуры нового gTLD (а не владельца доменного имени или регистратора). Существует три PDDRP:

Процедура разрешения разногласий в отношении товарных знаков после делегирования (TM-PDDRP) позволяет владельцу товарного знака подать иск против оператора регистратуры за участие в незаконном использовании товарных знаков в случае с gTLD верхнего или второго уровня.

Если речь идет о верхнем уровне, истец должен представить «четкое и убедительное свидетельство» того, что «действия оператора регистратуры при управлении и использовании нового gTLD, идентичного или сходного до степени смешения с товарным знаком истца, являются причиной или материально способствуют тому, что данный gTLD: (1) обеспечивает получение несправедливого преимущества вследствие различительной способности или репутации товарного знака истца; (2) наносит ущерб различительной способности или репутации товарного знака истца; (3) создает возможность смешения со знаком истца» (раздел 6.1 TM-PDDRP).

Если речь идет о втором уровне, истцы должны представить «четкое и убедительное свидетельство» того, что «действия оператора регистратуры указывают на: (а) недобросовестное поведение или практику оператора регистратуры, направленную на получение прибыли от продажи доменных имен, в которых незаконно используются товарные знаки; (б) злой умысел оператора регистратуры, направленный на получение прибыли от систематической регистрации доменных имен в gTLD, идентичных или сходных до степени смешения со знаком истца, что влечет за собой: (i) получение несправедливого преимущества вследствие различительной способности или репутации товарного знака истца; (ii) нанесение ущерба различительной способности или репутации товарного знака истца; (iii) создание сходства до степени смешения со знаком истца» (раздел 6.2 TM-PDDRP).

Если экспертная комиссия признала оператора регистратуры виновным, может быть рекомендовано несколько средств защиты прав, в том числе меры по предотвращению дальнейшей регистрации имен, в которых незаконно используются товарные знаки, приостановка регистрации новых доменных имен в соответствующем gTLD до прекращения нарушений или на предписанный экспертом фиксированный период времени или расторжение соглашения об администрировании домена верхнего уровня — при особых обстоятельствах, если оператор регистратуры действовал «со злым умыслом» (раздел 18 TM-PDDRP). В конечном счете, полномочиями на применение надлежащих средств защиты прав, если таковые будут признаны необходимыми, располагает ICANN.

На данный момент для разрешения разногласий посредством TM-PPDRP ICANN утверждены следующие поставщики услуг: Азиатский центр разрешения разногласий в отношении доменных имен (ADNDRC), Национальный арбитражный форум (NAF) и Всемирная организация по охране интеллектуальной собственности (ВОИС).

Процедура разрешения разногласий в отношении ограничений регистратур (RRDRP) позволяет официальному учреждению подать иск против оператора регистратуры нового gTLD от сообщества за несоблюдение ограничений в отношении регистрации, описанных в его соглашении об администрировании домена верхнего уровня. Чтобы истец был признан выигравшей стороной, ему необходимо представить «наличие более веских доказательств» того, что: «(i) упомянутое подающей возражение стороной сообщество является определенным сообществом; (ii) имеется тесная связь между упомянутым сообществом и строкой или меткой gTLD; (iii) оператор TLD нарушил ограничения сообщества, описанные в его соглашении; (iv) истцу и указанному подающей возражение стороной сообществу нанесен измеримый ущерб». Средства защиты прав, рекомендуемые экспертной группой, аналогичны описанным для TM-PDDRP. В конечном счете, полномочиями на применение этих средств защиты прав располагает ICANN.

Процедура разрешения споров в области обеспечения общественных интересов (PICDRP) позволяет любому лицу или организации (далее — «отправитель») подать иск против оператора регистратуры нового gTLD за несоблюдение обязательства или обязательств по обеспечению общественных интересов, изложенных в спецификации 11 его соглашения об администрировании домена верхнего уровня. Отправитель должен отправить в ICANN «сообщение о нарушении PIC», заполнив опубликованную в интернете форму. В «сообщении о нарушении PIC» требуется: (1) указать PIC, являющиеся основанием для сообщения; (2) обосновать обвинения в несоблюдении одного или нескольких PIC и представить подтверждающие доказательства; (3) указать, каким образом в результате предполагаемого несоблюдения обязательств пострадал отправитель. ICANN может проверить соблюдение или созвать «Постоянную комиссию». Если будет выявлено несоблюдение оператором регистратуры своих PIC, ему предоставляется 30 дней на устранение нарушений. Если оператор регистратуры не решит проблемы с несоблюдением, ICANN определит надлежащие средства защиты прав.

5.2.2.5 Депозитарий товарных знаков (TMCH)

TMCH — это созданная в марте 2013 года централизованная база проверенных товарных знаков всего мира, которой ICANN поручила защищать владельцев товарных знаков в новых gTLD. TMCH выполняет несколько важных функций, в числе которых аутентификация и проверка регистрационных записей товарных знаков, хранение этих записей в базе данных и передача этой информации регистраторам и регистратурам новых gTLD. Информация, содержащаяся в TMCH, является опорой для механизмов защиты прав, таких как Служба ранней регистрации (благодаря которой владельцы товарных знаков могут регистрировать доменные имена, соответствующие своим товарным знакам, прежде чем те станут общедоступными) и Служба обработки претензий в отношении товарных знаков (обеспечивающая отправку владельцам доменов и товарных знаков уведомлений о регистрации доменных имен, в которых незаконно используются товарные знаки). Регистрация товарного знака в TMCH необходима не только для участия в ранней регистрации и использования Службы обработки претензий в отношении товарных знаков, но и для использования других механизмов защиты прав конкретных регистратур, таких как

механизмы блокирования доменных имен, например, Списка защищенных меток доменов (DPML) компании Donuts; однако есть и такие RPM (например, URS), для которых это необязательно. Таким образом, TMCH — важный инструмент защиты прав на товарные знаки в рамках программы New gTLD.

5.2.3 Рассмотрение этих механизмов: способствовали ли они решению проблем с защитой прав на товарные знаки и потребителей в условиях расширения пространства gTLD?

Группа по анализу CCT занялась изучением вопроса о том, помогли ли эти механизмы решить проблемы, связанные с защитой прав на товарные знаки и потребителей в условиях расширения пространства gTLD, и постаралась получить данные для оценки воздействия программы New gTLD ICANN на стоимость и объем работы, необходимой для защиты товарных знаков в системе доменных имен.

Группа по анализу CCT в первую очередь обратилась к данным, полученным ICANN в составе отчетов по показателям CCT,¹¹⁶ но также воспользовалась выполненным INTA исследованием воздействия,¹¹⁷ где надеялась обнаружить дополнительные данные о воздействии новых gTLD на расходы владельцев брендов, а также данными и комментариями, полученными во время анализа механизмов защиты прав ICANN. Кроме того, группа по анализу CCT обратила внимание на параллельную деятельность рабочих групп, в настоящее время изучающих механизмы защиты прав, стремясь не мешать этой деятельности и не дублировать ее, и ждет возможности ознакомиться с отчетами этих групп.

5.2.3.1 Анализ механизмов защиты прав (RPM) ICANN

Предварительные выводы по результатам анализа механизмов защиты прав (RPM) ICANN, выполненного корпорацией ICANN (отчет представлен 11 сентября 2015 года), заключаются в том, что в целом URS в отдельных случаях привела к положительным результатам. Скорость и низкая стоимость отвечает потребностям лиц, чьи случаи очевидны, которых устраивает простая приостановка действия доменного имени. Однако некоторые правообладатели не воспользовались этой службой из-за того, что сочли «четкое и убедительное свидетельство» слишком строгой нормой, при том что средства правовой защиты URS ограничены приостановкой действия. Также выражалась озабоченность по поводу возможности повторной регистрации доменного имени другим потенциальным нарушителем, после того как оно станет доступным, поэтому некоторым правообладателям было бы удобнее иметь это доменное имя в собственном портфеле, а этого можно добиться посредством UDRP. Действительно, приостановка действия доменного имени имеет сомнительную ценность.

5.2.3.2 Выполненное INTA исследование воздействия

Результаты выполненного Международной ассоциацией по товарным знакам (INTA) исследования воздействия содержат важные сведения, которые более полно

¹¹⁶ ICANN, «Отчетность по показателям конкуренции, потребительского доверия и потребительского выбора (CCT)», дата просмотра — 10 октября 2017 года, <https://www.icann.org/resources/reviews/cct/metrics>

¹¹⁷ Nielsen (апрель 2017 года), опрос INTA для оценки воздействия новых gTLD на расходы, дата просмотра — 24 октября 2017 года, community.icann.org/download/attachments/56135378/INTA_Cost_Impact_Report_revised_4-13-17_v2.1.pdf

информируют сообщество о воздействии программы New gTLD ICANN на стоимость и объем необходимых усилий по защите товарных знаков в DNS. Члены INTA и владельцы интеллектуальной собственности неоднократно выражали озабоченность в связи с созданием новых gTLD на том основании, что это расширение скорее всего приведет к дополнительным повышенным расходам на защиту прав на интеллектуальную собственность. Был проведен опрос, чтобы оценить, какие дополнительные расходы и усилия потребовались для защиты товарных знаков в DNS. INTA — всемирная организация, объединяющая 6 600 владельцев товарных знаков и специалистов более чем из 190 стран. В связи с этим она является подходящим участником опроса, проведенного компанией Nielsen на основе предложений CCTRT. При этом членов INTA попросили указать все свои расходы за прошедшие 2 года (2015 год и 2016 год). В состав этой сметы расходов входят:

- внутренние и внешние расходы на юридическое сопровождение,
- регистрационные пошлины,
- расходы на расследование,
- общий размер расходов, включая неденежные выплаты, на оплату труда персонала, отвечающего за эти виды деятельности.

Респонденты, принявшие участие в этом опросе, сообщили, что сбор данных для подготовки необходимых ответов был трудной задачей. В общей сложности приняли участие 33 респондента, в том числе одна некоммерческая организация. Хотя процент участников опроса на самом деле превышает типовое значение для аналогичной выборки,¹¹⁸ особенно с учетом необходимых усилий по заполнению сложной анкеты, со статистической точки зрения размер выборки опрошенных мал, поэтому при интерпретации результатов следует проявлять некоторую осторожность. Тем не менее, результаты позволяют выделить наиболее важные темы и тенденции.¹¹⁹

Основные выводы по результатам исследования воздействия:

1. Хотя одна из целей программы New gTLD — расширение выбора, для владельцев брендов выбор, по-видимому, не является главной причиной регистрации ими новых gTLD. Напротив, главной причиной регистрации доменных имен в новых gTLD для подавляющего большинства (90%) владельцев товарных знаков является стремление защититься — не допустить регистрации доменного имени другим лицом.
2. Для доменных имен, зарегистрированных владельцами брендов в новых gTLD, обычно используется услуга паркинга, и такие имена не представляют иной ценности, кроме предотвращения их несанкционированного использования другими лицами.
3. Программа New gTLD привела к увеличению общих расходов на защиту товарных знаков. При этом расходы на мониторинг интернета и переадресацию являются самой крупной статьей расходов. Эти расходы в одинаковой степени затронули крупные и мелкие компании. Наиболее значимый для увеличения затрат фактор — количество брендов.

¹¹⁸ Данное утверждение сделано на основании общего опыта работы компании Nielsen с выборками клиентов или членов.

¹¹⁹ По мнению компании Nielsen, суммарный размер выборки достаточен для получения данных о направлении этих тенденций, однако конкретные значения могут содержать большую погрешность (отклонение процентного значения в большую или меньшую сторону, о котором постоянно упоминается при проведении опросов).

4. Респонденты сообщили, что средние общие издержки правоприменения, связанные с доменами верхнего уровня в целом (как существовавшими ранее, так и новыми), на одну компанию составляют \$150 000 в год. С другой стороны, эти расходы участников опроса варьировались в широких пределах.¹²⁰ Указанное обстоятельство заслуживает дополнительного изучения при проведении будущих опросов.
5. Что касается споров, более чем 75% поданных к настоящему моменту исков связаны с услугами сохранения конфиденциальности и регистрации через доверенных лиц, и почти в 2/3 случаях данные WHOIS в том или ином отношении были недостоверными или неполными.
6. Хотя на долю новых gTLD приходится 1/6 часть издержек правоприменения, количество таких имен пока еще меньше 1/6 части всех зарегистрированных доменных имен. Другими словами, доля издержек правоприменения, относящихся к новым gTLD, примерно равна 18% от общей суммы издержек правоприменения для TLD, в то время как общее количество зарегистрированных новых gTLD составляет 10% от всех TLD на момент исследования воздействия.¹²¹ Эти данные свидетельствуют о непропорционально большой доле расходов на правоприменительные действия, связанные с новыми gTLD, в составе общих расходов на правоприменительные действия. Следовательно, имеется еще одно свидетельство того, что в новых gTLD пропорционально чаще незаконно используются товарные знаки, чем в существовавших ранее gTLD.¹²²
7. В целом считается, что механизмы защиты прав помогли снизить ожидаемые риски создания новых gTLD. Ответы на вопрос: «Сообщите, почему вы считаете, что перечисленные выше механизмы защиты прав снизили или не снизили риски, связанные с новыми TLD?» были разнообразными, но позволили лучше понять образ мыслей участвовавших в опросе владельцев брендов.¹²³ Две трети опрошенных

¹²⁰ Диапазон указанных общих расходов варьировался от нуля до \$5,2 млн.

¹²¹ Nielsen, опрос для оценки воздействия новых gTLD на расходы (2017 год). Средние затраты для всех TLD за 2 года = \$292 000. Средние затраты для новых gTLD за 2 года = \$53 690 (приблизительно 18%).

¹²² Nielsen, опрос для оценки воздействия новых gTLD на расходы (2017 год). «Компания Nielsen разъясняет, что указанные затраты на мониторинг интернета, являющиеся одной из главных статей расходов, следует использовать в ограниченных пределах — эти расходы носят общий характер и относятся не только к новым gTLD. Организация оплачивает мониторинг всех TLD. Скорее всего расходы на мониторинг постепенно увеличиваются, учитывая необходимость дополнительно отслеживать новые gTLD, и действительно есть неофициальные свидетельства того, что после создания новых gTLD большее число владельцев брендов начало заниматься мониторингом. Однако эти расходы не были детализированы в анкете опроса. По существу, мониторинг рассматривался как безвозвратные издержки. Таким образом, целесообразно предположить, что указанные расходы выросли, а не сократились». Следовательно, общий размер расходов, вероятно, превышает 18%».

¹²³ «Период ранней регистрации — часто сопряжен для владельца бренда с крупными расходами; Период требований — мы получаем уведомление уже после регистрации доменного имени; URS — имя не передается новому владельцу; узкие критерии для действий; PDDRP — установлены настолько узкие критерии, что вероятность возникновения подобных обстоятельств чрезвычайно мала; UDRP — критерии четко определены; имеется полезное прецедентное право; одним из вариантов является передача имени новому владельцу. Однако цена — сдерживающий фактор во всех случаях, кроме наиболее вопиющих. Периоды ранней регистрации и рассмотрения претензий в отношении товарных знаков слишком короткие; компаниям приходится принимать дополнительные меры, чтобы следить за своим портфелем в многочисленных gTLD, появляющихся еженедельно.

Некоторые мы используем, и они приносят пользу. Другие нет.

URS: слишком дорого для простой приостановки действия (без передачи) домена, являющегося предметом спора; Процедуры после делегирования: очень интересны, но сложны и с трудом приводятся в действие (практически, необходимы совместные действия различных владельцев TM).

Периоды ранней регистрации малоэффективны, потому что многие регистратуры устанавливают для владельцев брендов дискриминационные цены, хотя в то же время многие предлагают такое же доменное имя

респондентов считают, что процедуры UDRP и обязательные периоды ранней регистрации способствовали снижению рисков. При этом 90% респондентов в период Sunrise зарегистрировали доменные имена в новых gTLD. Доли тех, кто считает механизмы защиты прав эффективными, распределились следующим образом:

- а. Период ранней регистрации 79%
- б. UDRP 73%
- в. Период требований 66%
- г. URS 49%
- д. PDDRP/RRDRP/PICDRP 27%

Тем не менее, есть достаточно солидный объем неофициальных доказательств того, что владельцы брендов неохотно покупают доменные имена в периоды ранней регистрации. При этом многие считают их чрезмерно дорогими:

«Периоды ранней регистрации очень быстро превратились из средства защиты в источник прибыли»¹²⁴

«Периоды ранней регистрации малоэффективны, потому что многие регистратуры устанавливают для владельцев брендов дискриминационные цены, хотя в то же время многие предлагают такое же доменное имя лицам, не являющимся владельцами брендов, по гораздо более низкой цене».¹²⁵

«Регистратура .top увеличила размер сбора за раннюю регистрацию [компания].top до \$30 000. Мы отказались от регистрации»¹²⁶

1. Регистрацией в TMCH воспользовалось большинство респондентов. Если обратиться к данным, большая часть респондентов (примерно 9 из 10) зарегистрировала в TMCH хотя бы 1 товарный знак. При этом 6 из 10

лицам, не являющимся владельцами брендов, по гораздо более низкой цене. Уведомления о претензиях не мешают сквоттерам регистрировать доменные имена, несмотря на уведомление о существующих правах. Это означает, что после регистрации в новых gTLD сохраняются те же проблемы, что и в TLD, существовавших ранее. URS предусматривает более тяжелое бремя доказывания, чем менее эффективная с точки зрения затрат UDRP. PDDRP, RRDRP и PICDRP могут быть эффективными, однако возможности их применения понимаются недостаточно хорошо, вследствие чего они мало влияют на снижение рисков. Мы преимущественно занимались защитными регистрациями.

Это хорошие, но неполные механизмы. URS быстрее UDRP, но не является «вопросом нескольких дней» — неэффективна в случае действительно вредоносного ПО и не позволяет получить доменное имя. Для UDRP требуется несколько месяцев. Обе процедуры дорогие. Компаниям все еще необходимо осуществлять защитную регистрацию по высокой цене, чтобы уберечь своих клиентов от неправомерного использования наших брендов, пользующихся доверием.

Мы предпочли бы использовать для товарных знаков блокирующую процедуру, которая позволила бы резко снизить риски, но в отсутствие возможности блокирования TMCH по крайней мере предоставляет нам механизм регистрации доменов, соответствующих товарным знакам, прежде чем они будут перехвачены киберсквоттерами. Процедура обработки претензий в TMCH оказывает небольшое воздействие, потому что охватывает весьма ограниченный период времени. Мы считаем, что URS имеет ограниченную ценность, поскольку ее необходимо использовать для нескольких доменов. Мы используем UDRP, но только для существовавших ранее TLD, так как подавляющее количество доменов, нарушающих права, регистрируется в зоне .com.

Период ранней регистрации позволяет владельцам товарных знаков купить домен, содержащий основной товарный знак, раньше других. Однако другие механизмы, по-видимому, не настолько эффективны и требуют выделения владельцами товарных знаков существенных ресурсов.

У нас не было возможности воспользоваться.

Владельцы доменов готовы рискнуть небольшой суммой, уплатив регистрационный сбор, чтобы использовать доменное имя, в состав которого входит общеизвестный товарный знак». (стр. 59).

¹²⁴ Nielsen, опрос для оценки воздействия новых gTLD на расходы (2017 год), стр. 52.

¹²⁵ Тот же источник, стр. 59.

¹²⁶ Тот же источник, стр. 50.

зарегистрировали от 1 до 10 товарных знаков. Что касается соответствующих расходов респондентов, они широко варьируются от менее чем \$1 000 до \$48 000; при этом средние расходы составляют примерно \$7 700.

2. Созданная процедура URS стала альтернативой UDRP, но используется в меньшем объеме. К наиболее часто упоминавшимся причинам ее более низкой популярности относятся невозможность передачи доменного имени после принятия решения в пользу истца и более тяжелое бремя доказывания.
3. Что касается цен с набавкой, три четверти респондентов упоминали о том, что в некоторых случаях встречались с такими ценами на доменные имена, и на 2/3 их решений о регистрации доменных имен стратегия высоких цен оказала воздействие. При этом .sucks упоминался большинством как TLD, в котором респонденты уплачивали цену с надбавкой. Однако 15% респондентов полностью отказались приобретать доменные имена с надбавкой.

5.2.4 Отчет ICANN о показателях конкуренции, потребительского доверия и потребительского выбора (CCT)

5.2.4.1 Количество поданных исков (UDRP и URS)

Полученные ICANN данные по всем поставщикам услуг разрешения разногласий в отношении доменных имен,¹²⁷ ясно свидетельствуют, что общее количество поданных исков (UDRP + URS) существенно выросло после создания новых gTLD. Что касается UDRP, количество поданных исков UDRP довольно существенно выросло, в то время как URS использовалась в более ограниченном объеме и наблюдалось небольшое сокращение числа поданных исков за период, прошедший после введения этой службы и ее первого использования в новых gTLD в 2014 году. Первые новые gTLD появились в корневой зоне в 2013 году.¹²⁸ Однако только в 2014 году UDRP впервые была использована для нового gTLD — «Иск Canyon Bicycles GmbH против Domains By Proxy, LLC / Rob van Eck» — и решение по доменному имени <canyon.bike> было принято¹²⁹ 14 марта 2014 года. Первое решение в рамках URS по доменному имени <aeropostale.uop> было принято 28 апреля 2014 года.¹³⁰ Если взять за отправную точку предыдущий год, когда не было ни одного спора по новым gTLD, то в общей сложности были приняты решения по 3 371 спору, которые все рассматривались согласно UDRP и относились только к существовавшим ранее gTLD.

¹²⁷ ICANN, «Отчет о показателях конкуренции, потребительского доверия и потребительского выбора (CCT): механизмы защиты прав», дата просмотра — 10 октября 2017 года, <https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.12>

¹²⁸ ICANN, «Первые регистратуры новых gTLD получают токены для системы управления корневой зоной» («First New gTLD Registries Receive Tokens for Root Zone Management System»), дата просмотра — 10 октября 2017 года, <https://newgtlds.icann.org/en/announcements-and-media/announcement-22oct13-en>. Первые новые gTLD появились в корневой зоне в октябре 2013 года.

¹²⁹ Центр арбитража и урегулирования споров ВОИС, «Решение административной комиссии по иску Canyon Bicycles GmbH против Domains By Proxy, LLC / Rob van Eck, дело № D2014-0206», дата просмотра — 10 октября 2017 года, <http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2014-0206>, первое решение по новому gTLD, принятое в рамках UDRP.

¹³⁰ ADR, «Решение Национального арбитражного форума по апелляции в рамках процедуры URS: Aeropostale Procurement Company, Inc. против Майкла Кинси (Michael Kinsey) и других. Номер требования: FA1403001550933», дата просмотра — 10 октября 2017 года, <http://www.adrforum.com/Domaindecisions/1550933A.htm>, первое решение по новому gTLD, принятое в рамках URS.

Таблица 13: Количество исков, полученных поставщиками UDRP и URS.

[Обновлялось ежеквартально] [По состоянию на: 3 августа 2017 года]

Год	Общее количество (отдельно UDRP и URS)	Суммарное количество дел
2013	3 371 (UDRP)	3 371
2014	4 056 (UDRP) и 231 (URS)	4 287
2015	4 130 (UDRP) и 213 (URS)	4 343
2016	4 368 (UDRP) и 222 (URS)	4 590
2017, 1-й кв./2-й кв.	2 112 (UDRP) и 104 (URS)	2 216 (прим.: за первую половину года)

Источник: базы данных поставщиков арбитражных услуг
Категория проверки ССТ: потребительское доверие

В 2014 году общее количество исков (UDRP и URS в совокупности) увеличилось до 4 287, что соответствует приросту на 27%. В 2015 году общее количество исков снова незначительно выросло до 4 343 (это на 1,3% больше, чем в 2014 году), а в 2016 году еще на 5,7%, в результате чего общее количество исков составило 4 590. Таким образом, при сравнении общего количества исков в 2013 году, за год до рассмотрения первого спора по новому gTLD, и в 2016 году наблюдается существенный рост на 36% количества исков, полученных всеми поставщиками.

Если рассматривать только иски UDRP, за период с 2013 по 2014 год их количество выросло на 20%, затем в период с 2014 по 2015 год еще на 2%, а в период с 2015 по 2016 год на 5,8%. Если рассматривать отдельно иски URS, прежде всего следует отметить, что их популярность как RPM была и остается низкой: 231 иск в 2014 году, 213 исков в 2015 году и 222 иска в 2016 году. То есть на долю URS приходится всего лишь около 5% от общего числа поданных исков. Кроме того, по-видимому, отсутствует существенный рост количества исков из года в год. В 2015 году количество поданных исков URS сократилось по сравнению с 2014 годом, и даже в 2016 году общее количество исков URS не превысило их количества в 2014 году — в первом году работы новых gTLD. Это дает основание сомневаться в том, что данный механизм можно использовать как полезный RPM.

Важно отметить, что количество исков, поданных в рамках UDRP и URS, отражает лишь часть затрат владельцев товарных знаков на защиту своих брендов, и основная часть издержек правоприменения может иметь форму защитных регистраций/блокирования/наблюдения/отправки писем-предупреждений и судебного преследования — в настоящее время мы не располагаем данными об этом. Однако выполненное INTA исследование воздействия позволяет получить об этом некоторое представление.

5.2.4.2 Жалобы в ICANN на неисполнение решений UDRP и URS

Роль ICANN заключается в обеспечении соблюдения регистраторами UDRP и Правил UDRP, а также правил и процедуры URS.

Например, поставщик услуг UDRP согласно UDRP может подать жалобу на несоблюдение регистратором сроков блокирования домена, являющегося предметом разбирательства UDRP, или сроков ответа на отправленный поставщиком запрос на

подтверждение. При этом истец может подать жалобу в ICANN, если регистратор своевременно не привел в исполнение решение UDRP.

Что касается URS, к примеру, оператор регистратуры также должен своевременно заблокировать и в надлежащих случаях приостановить действие доменного имени в соответствии с постановлением, процедурами и правилами URS. Чтобы выдвинуть обвинение в подобных нарушениях выигравший разбирательство URS истец и поставщик услуг URS в соответствии с правилами URS могут подать в ICANN жалобу, заполнив веб-форму, предусмотренную отделом соблюдения обязательств для URS.

Судя по количеству поданных в ICANN жалоб на неисполнение решений UDRP и URS,¹³¹ число таких жалоб, относящихся к решениям в рамках UDRP, снизилось за период с 2012 по 2014 год примерно на 65%, и после этого оставалось практически неизменным, на уровне от 250 до 227 жалоб ежегодно. Количество жалоб, относящихся к URS, в 2014 году (в первом году, когда URS стала доступна для новых gTLD) было относительно большим, но в последние два года (2015 и 2016 годы) количество подобных жалоб уменьшилось примерно наполовину.

Таблица 14: Общее количество жалоб, поступивших в ICANN в рамках UDRP/URS¹³²

Год	Жалобы UDRP	Иски URS
2012	658	
2013	408	
2014	227	19
2015	250	11
2016	235	9
2017, 1-й кв./2-й кв.	122	10

Таблица 15: Сравнение % жалоб, поданных в ICANN по каждому RPM, с общим количеством решений по доменным именам, принятых в рамках каждого RPM

Год	URS	UDRP
2014	8%	5,5%
2015	5,1%	6%
2016	4%	5,4%

В 2014 году, когда стала доступна URS, ICANN получила относительно много жалоб. Если сравнивать с общим количеством дел, рассмотренных в том году в рамках URS, значение данного показателя составило 8%. При этом в 2014 году аналогичный показатель для UDRP составил 5.5%. Большая доля жалоб на неисполнение решений URS по сравнению с UDRP может быть обусловлена рядом факторов, включая относительную новизну, сложность процесса и его недавнее внедрение регистраторами.

При сравнении данных за 2015 и 2016 годы наблюдается уменьшение относительного количества жалоб на неисполнение решений URS, а в 2016 году таких жалоб фактически было меньше, чем для UDRP — 4%, по сравнению с 5,4% для UDRP.

¹³¹ Следует отметить, что жалобы, связанные с обоснованностью решений, выходят за рамки договорных полномочий ICANN.

¹³² ICANN, «Отчет о показателях конкуренции, потребительского доверия и потребительского выбора (CCT): механизмы защиты прав», дата просмотра — 18 октября 2017 года, <https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.9.b>

Возможно, с течением времени регистраторы, регистратуры и конечные пользователи разобрались в сложностях URS.¹³³

5.2.4.3 Депозитарий товарных знаков (ТМЧН)

ICANN поручила Analysis Group провести независимую проверку услуг ТМЧН на основе поступившей от Правительственного консультативного комитета (GAC) в мае 2011 года рекомендации провести комплексную проверку Депозитария товарных знаков после начала его работы.¹³⁴ Эта проверка была направлена на оценку сильных и слабых сторон услуг ТМЧН в свете указанной рекомендации и проводилась на основе анализа данных, полученных от ТМЧН и из сторонних источников, а также результатов интервьюирования и опроса заинтересованных сторон ТМЧН. Пересмотренный отчет,¹³⁵ в котором были отражены полученные во время общественного обсуждения комментарии к первоначальному отчету, а также результаты выполненного анализа, был опубликован 25 июля 2016 года.¹³⁶ Согласно отчету, полученные данные позволили сформулировать содержательные замечания касательно использования исследуемых услуг ТМЧН. Однако в этом исследовательском отчете отсутствовали данные об издержках и выгодах использования услуг ТМЧН в их текущем виде. На самом деле для оценки потенциальных издержек и выгод расширения или изменения спектра предоставляемых услуг был необходим конкретный анализ затрат и эффективности, который выходил за рамки отчета Analysis Group.

Краткое изложение выводов

Что касается возможности продлить период требований или расширить критерии совпадения, используемые для отправки уведомлений в период требований, в отчете было указано, что это принесет ограниченную пользу владельцам товарных знаков. В действительности такое расширение могло бы повлечь за собой рост расходов других групп заинтересованных сторон, таких как регистратуры, регистраторы и владельцы доменов, не имеющие товарных знаков. Ограниченный объем данных не позволил сделать какие-либо определенные выводы.

В отчете отмечалось, что, поскольку анализ издержек и выгод не был выполнен, при возможном расширении службы обработки претензий или критериев совпадения следует учесть неизбежные компромиссы, необходимость которых ощущают различные группы заинтересованных сторон. Действительно, в этом отчете подчеркивалось, что при анализе необходимости продлить период требований, нужно оценить воздействие такого продления на потенциальное количество регистраций. Эффективность уведомлений службы обработки претензий зависит от количества предпринятых попыток регистрации; если таких попыток мало, то и потенциальное количество регистраций с нарушениями сокращается.

¹³³ ICANN, «Отчет о показателях конкуренции, потребительского доверия и потребительского выбора (CCT): механизмы защиты прав», дата просмотра — 4 марта 2017 года, <https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en>

¹³⁴ ICANN (26 мая 2011 года), Комментарии GAC к Руководству кандидата (в редакции от 15 апреля 2011 года), дата просмотра — 15 октября 2017 года, <https://archive.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf>

¹³⁵ Analysis Group, пересмотренный отчет о независимой проверке Депозитария товарных знаков (ТМЧН), 2017 год.

¹³⁶ Analysis Group, проект отчета о независимой проверке Депозитария товарных знаков (ТМЧН), июль 2016 года, дата просмотра — 10 октября 2017 года, <https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf>

В отчете содержится вывод, что после окончания 90-дневного периода обработки претензий регистрационная деятельность идет на спад, поэтому расширение периода требований на несколько месяцев, вероятно, принесет мало пользы.

Кроме того, в отчете указано, что по имеющимся данным владельцы товарных знаков, по-видимому, испытывают меньшую озабоченность в отношении использования различных вариантов строк, соответствующих товарным знакам, и, следовательно, расширение критериев совпадения принесет правообладателям небольшую пользу. Напротив, потенциальный ущерб владельцам доменов, у которых нет товарных знаков, может вырасти. Последние могут оказаться в ситуации, когда придется отказаться от регистрации разновидности строки, соответствующей товарному знаку, которая не считалась бы незаконным использованием товарных знаков.

Наконец, в отчете был рассмотрен период ранней регистрации и ответы на вопросы анкеты. По-видимому, хотя владельцы товарных знаков признали ценность периода ранней регистрации и многие действительно его используют, многие владельцы после регистрации своих товарных знаков в ТМСН фактически не участвуют в ранней регистрации. В отчете сделан вывод, что причиной этому может быть стоимость ранней регистрации доменных имен или то, что другие услуги ТМСН по защите правообладателей, такие как услуги обработки претензий, уменьшают необходимость использования ранней регистрации владельцами товарных знаков. Группа по анализу ССТ считает, что это также может происходить из-за огромного количества новых gTLD. Стоимость защитных регистраций, помноженная на большое количество новых gTLD, становится непомерно дорогой, и немногие владельцы брендов готовы заниматься столь широкомасштабной защитной регистрацией доменных имен. Группа по анализу ССТ задала вопрос, действительно ли дополнительные расходы на услуги ТМСН приносят пользу, а не служат сами по себе сдерживающим фактором, создавая необходимость дополнительных расходов со стороны владельцев брендов.

5.2.4.4 Процедура разрешения разногласий в отношении товарных знаков после делегирования (TM-PDDRP)

В отдел соблюдения договорных обязательств ICANN не поступало жалоб на несоблюдении операторами регистратур PDDRP. Однако следует отметить, что в настоящее время рабочая группа GNSO ведет процесс разработки политики (PDP) для пересмотра всех механизмов защиты прав во всех gTLD, изучая возможные препятствия для реализации PDDRP, поскольку на сегодняшний день неизвестны случаи подачи исков в рамках PDDRP через таких поставщиков.

5.2.4.5 Решения по процедуре разрешения разногласий в отношении ограничений регистратур (RRDRP)

RRDRP предназначена для использования в тех ситуациях, когда оператор регистратуры нового gTLD от сообщества не соблюдает ограничения регистрации, изложенные в его соглашении об администрировании домена верхнего уровня. По состоянию на 3 августа 2017 года не было зарегистрировано ни одного иска в рамках RRDRP.

5.2.4.6 Доля ранних регистраций и заблокированных доменов в общем количестве регистраций для каждого TLD

По состоянию на 3 августа 2017 года сведения о количестве ранних регистраций в сравнении с общим количеством зарегистрированных новых gTLD поступили только от ICANN. По данным ICANN сводная информация о предлагаемых регистратурами коммерческих услугах блокирования отсутствует. Группа по анализу конкуренции, потребительского доверия и потребительского выбора (CCTRT) по-прежнему готова принять любые подобные данные.

Заключение

Имеющиеся в нашем распоряжении данные несомненно указывают на увеличение количества споров после создания новых gTLD, при этом количество споров после создания новых gTLD растет из года в год. Действительно, в 2016 году общее число поданных исков (UDRP и URS в совокупности) увеличилось на 36% по сравнению с 2013 годом, когда в корневой зоне появились первые новые gTLD. (На 25%, если использовать в качестве отправной точки среднее количество за 2012 и 2013 годы.)

Однако рост количества разногласий в отношении доменных имен сам по себе не вызывает удивления, так как объемы регистрации доменных имен во всем мире продолжают увеличиваться по мере появления в корневой зоне новых gTLD и начала регистрации соответствующих доменных имен. Гораздо уместнее спросить, наблюдается ли пропорционально больший рост объемов незаконного использования товарных знаков в новых gTLD по сравнению с TLD, существовавшими ранее. Ответить на этот вопрос сложнее, поскольку при оценке незаконного использования товарных знаков нужно учитывать множество факторов, и в некоторых случаях необходимые данные могут просто отсутствовать. Выполненное INTA исследование воздействия — хороший пример того, насколько сложно получить такую информацию.

Помимо UDRP и URS владельцы товарных знаков также могут использовать множество других средств для борьбы с неправомерной регистрацией доменных имен, таких как судебное преследование и отправка писем-предупреждений. Эти действия не отслеживаются централизованно, а также отсутствуют сведения о связанных с ними расходах. Отслеживание или попытка отслеживать такие данные не входит в круг задач ICANN. Однако ICANN действительно получает данные об использовании механизмов разрешения споров, UDRP и URS, от всех поставщиков услуг урегулирования разногласий в отношении доменных имен. Эти данные свидетельствуют о том, что количество разногласий в отношении доменных имен растет. Мы также получили от ICANN данные о количестве зарегистрированных новых gTLD по сравнению с общим количеством зарегистрированных gTLD (как существовавших ранее, так и новых gTLD). Эти данные также свидетельствуют об увеличении объемов регистрации доменных имен в gTLD. Однако в составе показателей ICANN отсутствует информация о сравнительном использовании UDRP, скажем, об использовании UDRP для новых gTLD в сравнении с использованием для существовавших ранее TLD.

Поэтому, чтобы попытаться ответить на вопрос, являются ли пропорционально большими объемы незаконного использования товарных знаков в новых gTLD по сравнению с объемами аналогичных нарушений в существовавших ранее TLD, можно обратиться к данным крупного поставщика услуг по разрешению споров, каковым является ВОИС, поскольку эти данные общедоступны.

Данные ВОИС за 2016 год демонстрируют, что количество споров, связанных с киберсквоттингом в новых gTLD, выросло до 16% от общего количества дел, рассмотренных ВОИС в 2016 году. При этом чаще всего одной из сторон спора в

отношении доменных имен были следующие gTLD: .XYZ, .TOP и .CLUB. Доля существовавших ранее gTLD в общем количестве рассмотренных ВОИС дел составила 70%. По сути, если обратиться только к данным ВОИС, 18,6% рассмотренных этой организацией дел по gTLD относилось к новым gTLD. Если обратиться к статистическим данным ICANN о количестве зарегистрированных доменных имен, то на конец 2016 года в gTLD было зарегистрировано 196 493 430 доменных имен, из которых 27 659 702 — новые gTLD. Таким образом, доля новых gTLD составляет 14% от общего объема зарегистрированных gTLD. Эти данные являются достаточно убедительным признаком того, что в настоящее время наблюдается пропорционально больший рост объемов незаконного использования товарных знаков в новых gTLD по сравнению с TLD, существовавшими ранее.

Возникает вопрос, насколько ценным механизмом защиты прав является URS, учитывая малые объемы использования этой службы по сравнению с UDRP. То обстоятельство, что TM-PDDRP и RRDRP для регистратур до настоящего времени ни разу не использовались, с одной стороны, может заставить сомневаться в их необходимости, но в равной степени также может подчеркивать, что само существование этих процедур является сдерживающим фактором.¹³⁷

5.2.5 Рекомендации

Рекомендация 40: Исследование воздействия для определения воздействия программы New gTLD на стоимость и объем усилий по защите товарных знаков в системе доменных имен, следует проводить регулярно, чтобы оценить изменение ситуации в долгосрочной перспективе, по мере развертывания программы New gTLD и увеличения количества регистраций новых gTLD. В частности, мы бы рекомендовали провести следующее исследование воздействия в течение 18 месяцев после опубликования итогового отчета CCTRT, а дальнейшие исследования проводить каждые 18–24 месяца. CCTRT признает тот факт, что это исследование было выполнено в 2017 году компанией Nielsen путем опроса членов INTA и рекомендует сохранить подобную практику, отмечая необходимость упростить участие в этих опросах.

¹³⁷ Источники:

Сводка источников информации о процедурах:

Вики-страница сообщества группы по анализу конкуренции, потребительского доверия и потребительского выбора, «Процедуры», дата просмотра — 5 марта 2017 года, <https://community.icann.org/display/CCT/Procedures>
ICANN, Анализ механизмов защиты прав.

GNSO ICANN, «PDP: пересмотр всех механизмов защиты прав во всех gTLD», дата просмотра — 5 марта 2017 года, <https://gns0.icann.org/en/group-activities/active/rpm>
Analysis Group, проект отчета о независимой проверке Депозитария товарных знаков (TMCH), июль 2016 года, дата просмотра — 5 марта 2017 года, <https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf>

Вики-страница сообщества группы по анализу конкуренции, потребительского доверия и потребительского выбора, «Процедуры», дата просмотра — 5 марта 2017 года, <https://community.icann.org/display/CCT/Procedures>.

Сводка источников информации о мерах защиты и обязательствах по обеспечению общественных интересов:

ICANN, «Отчет о показателях конкуренции, потребительского доверия и потребительского выбора (CCT): механизмы защиты прав», дата просмотра — 5 марта 2017 года, <https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en>

Обоснование/сопутствующие выводы: Издержки, вероятно, будут значительно меняться с течением времени, по мере делегирования новых gTLD и увеличения количества зарегистрированных доменных имен. Периодическое исследование воздействия позволило бы сравнивать показатели в динамике по времени.

Кому: Корпорации ICANN

Предварительное условие или уровень приоритета: Высокий

Консенсус в группе: Да

Подробности: Развитие в долгосрочной перспективе позволит составить более точную картину затрат по мере их изменения и отследить эффективность механизмов защиты прав в DNS в целом.

Критерии успеха: Результаты подобных исследований воздействия позволят получить значительный объем дополнительных данных для рабочих групп, в настоящее время изучающих механизмы защиты прав и ТМЧН, и для будущих рабочих групп, что принесет пользу всему сообществу. Рекомендации будущих групп по анализу CCT также могли бы видоизменяться надлежащим образом.

Рекомендация 41: Следует провести полный анализ URS и рассмотреть аспекты ее совместимости с UDRP. Однако с учетом того, что сейчас проводится PDP для пересмотра всех RPM во всех gTLD, во время указанного анализа нужно принять во внимание отчет о результатах этого процесса разработки политики, когда тот будет опубликован, и необходимость в таком анализе может отпасть, если отчет окажется достаточно содержательным в плане выводов и всесторонней оценки потенциальных изменений.

Обоснование/сопутствующие выводы: URS, похоже, используется не столь активно, как ожидалось, так что полезно будет понять причины этого явления и разобраться, считается ли URS эффективным механизмом предотвращения злоупотреблений. Также важно обеспечить, чтобы все gTLD находились в равных условиях. На самом деле, PDP по пересмотру всех механизмов защиты прав во всех gTLD, который осуществляется параллельно с работой этой группы по анализу CCT, внесет свой вклад в рассмотрение этого вопроса, так как соответствующий отчет должен быть опубликован в 2018 году. Отчет указанной рабочей группы необходимо принять к сведению при определении круга задач любой проверки и любых потенциальных изменений.

Кому: Организации поддержки доменов общего пользования

Предварительное условие или уровень приоритета: Предварительное условие

Консенсус в группе: Да

Подробности: При анализе URS рассматриваются, в частности: 1) необходимость предусмотреть в URS возможность передачи доменного имени, а не только приостановки действия; 2) необходимость продолжения работы двух систем (UDPR и URS параллельно) в полном объеме с учетом их сравнительной ценности; 3) потенциальная применимость URS ко всем gTLD; 4) вероятность возникновения путаницы для потребителей и правообладателей в связи с наличием разных механизмов для разных категорий gTLD.

Критерии успеха: Исходя из результатов, четкое общее представление о целесообразности использования URS и о том, насколько эффективно она работает в соответствии с первоначальным замыслом.

Рекомендация 42: Следует выполнить сравнительный анализ издержек и выгод, а также проверку ТМСН и круга его задач для сбора количественных данных об издержках и выгодах, связанных с текущим состоянием услуг ТМСН, что обеспечит возможность результативного пересмотра политики.

Обоснование/сопутствующие выводы: По-видимому, нужна всесторонняя проверка ТМСН, в том числе анализ издержек и выгод. Похоже, что эффективность работы ТМСН вызывает сомнение. Авторы пересмотренного отчета о независимой проверке услуг Депозитария товарных знаков (ТМСН)¹³⁸ не смогли сформулировать окончательные выводы из-за ограниченного объема данных и особо отметили, что им не удалось проанализировать соотношение издержек и выгод продления периода требований или расширения критериев совпадения. PDP по пересмотру всех RPM во всех gTLD, который осуществляется параллельно с работой этой группы по анализу ССТ, внесет свой вклад в рассмотрение этого вопроса, так как соответствующий отчет должен быть опубликован в январе 2018 года. Отчет указанной рабочей группы необходимо принять к сведению при определении круга задач любой проверки и любых потенциальных изменений.

Кому: Организации поддержки доменов общего пользования

Предварительное условие или уровень приоритета: Предварительное условие

Консенсус в группе: Да

Подробности: Похоже, что идет активное обсуждение того, стоит ли расширить сферу действия ТМСН, чтобы применять его не только в случае идентичных совпадений, и стоит ли включить формулу «метка + ключевое слово» или распространенные опечатки в этой метке. Если такое расширение считается полезным, то должны быть понятны его основания.

Критерии успеха: Доступность надлежащих данных для подготовки рекомендаций и эффективного анализа политики ТМСН.

¹³⁸ Analysis Group, пересмотренный отчет о независимой проверке Депозитария товарных знаков (ТМСН), 2017 год.

6 Приложения

6.1 Мнения меньшинства относительно документа о злоупотреблении DNS и рекомендации 4

Хотя CCT-RT смогла добиться единодушной поддержки большинства своих рекомендаций, некоторые члены RT не согласны с предложением создать процедуру разрешения споров при злоупотреблении DNS (DADRP). В настоящих документах с заявлениями изложены различные основания для такого несогласия:

1. CCT-RT решила руководствоваться тем принципом, что в основе анализа и рекомендаций будут лежать данные. Однако нет никаких данных, подтверждающих идею создания DADRP. Нет данных, указывающих на то, что операторы регистратур несут (прямую или косвенную) ответственность за злоупотребления в своих TLD; нет данных, указывающих на неспособность отдела соблюдения договорных обязательств ICANN обеспечивать выполнение требований договоров; а также нет данных, указывающих, что злоупотребление DNS со стороны определенных TLD направлено против конкретных третьих лиц, которые могли бы инициировать DADRP. Следовательно, эта рекомендация противоречит модели работы CCT-RT на основе данных.
2. Скорее наоборот, в отчете о злоупотреблении DNS четко указано, что попытка борьбы со злоупотреблением DNS через регистратуры DNS ошибочна и неэффективна. Ни одна из мер защиты, которые должны были принять операторы новых gTLD, по-видимому, никак не способствовала сокращению объемов распространенных злоупотреблений, а одна из них (внедрение DNSSEC) скорее всего привела к *увеличению* количества злоупотреблений. Тот факт, что борьба со злоупотреблениями через регистратуры DNS оказалась неэффективной, не должен вызывать удивление, поскольку у регистратур нет прямых связей с владельцами доменов и нет других механизмов, кроме приостановки работы домена для устранения злоупотреблений (что не во всех случаях является правильным подходом). DADRP, предусматривающая наказание регистратур за поведение владельцев доменов, которых регистратуры не контролируют и с которыми они не связаны, — принципиально ошибочный подход, который не решает проблему злоупотреблений в DNS.
3. Если есть сомнения в эффективности работы отдела соблюдения договорных обязательств ICANN по обеспечению соблюдения регистратурами своих договорных обязательств, этот вопрос следует решать путем совершенствования отдела соблюдения договорных обязательств ICANN, а не путем создания новой процедуры разрешения споров. Преимуществом подхода, заключающегося в совершенствовании отдела соблюдения договорных обязательств ICANN, является возможность решить проблемы во всем спектре договоров с регистратурами и регистраторами, в то время как создание DADRP в лучшем случае приведет к улучшению механизмов правоприменения в одной конкретной области. Создание уникальных процедур разрешения споров для отдельных разделов договора по своей сути не допускает масштабирования, и это невозможно сделать для всех главных компонентов договора. Не менее важно, что этот подход создает огромную неопределенность для связанных договорными обязательствами сторон,

которые могут оказаться в ситуации, когда третья сторона, даже в том случае, если ICANN рассмотрела проблему и пришла к выводу, что требования договора соблюдаются, вправе не согласиться с такой оценкой и по своей инициативе запустить дорогостоящую и сложную процедуру разрешения спора.

4. Хотя злоупотребление DNS — важная тема, в уставе группы по анализу CCT указано, что она только «изучит (A) степень, в которой расширение gTLD будет способствовать росту конкуренции, потребительского доверия и потребительского выбора, и (B) эффективность процесса подачи и оценки заявок в рамках раунда подачи заявок на новые gTLD и мер защиты, предусмотренных для устранения проблем, возникающих в связи с проведением раунда подачи заявок на новые gTLD». Следовательно, мы должны проанализировать существующие меры защиты, которые были введены для раунда 2012 года, но не должны разрабатывать совершенно новые механизмы борьбы со злоупотреблением DNS.

Jordyn Buchanan (Джордин Бьюкенен), Карлос Пауль Гутьеррес (Carlos Raul Gutierrez), Карлтон Сэмюэлс (Carlton Samuels), Ваудо Сиганга (Waldo Siganga)

6.2 Индивидуальное заявление

Джонатану Зуку (Jonathan Zuck)
председателю CCT-RT

Дрю Бэгли (Drew Bagley)
член руководства CCT-RT

25 октября 2017 года

По вопросу: Опубликование проекта рекомендаций для общественного обсуждения

Уважаемый председатель CCT-RT г-н Зук,

Хочу представить для вашего рассмотрения, а также для более широкого рассмотрения Группой по анализу конкуренции, потребительского доверия и потребительского выбора (CCT-RT) и сообществом, проект рекомендации (здесь и далее: «Рекомендация 5»), которая относится к выводам CCT-RT, содержащимся в настоящем проекте главы о злоупотреблении DNS. Рекомендация 5 не была включена в состав этой главы при подготовке документа к вынесению на общественное обсуждение, потому что CCT-RT не хватило времени для надлежащего обсуждения анализа и определения целесообразности утвердить эту рекомендацию до начала периода общественного обсуждения. Тем не менее, я прошу вас оформить Рекомендацию 5 как дополнение к проекту отчета, чтобы проинформировать сообщество о том, что такая рекомендация может быть дана, и предоставить адекватную возможность прокомментировать ее. CCT-RT смогла бы руководствоваться полученными комментариями во время будущего анализа данного предложения.

Искренне ваш,

Дрю Бэгли

Рекомендация 5: ICANN должна собрать и опубликовать данные о цепочке сторон, отвечающих за регистрацию доменных имен в gTLD.

Обоснование/сопутствующие выводы: В настоящее время отсутствует согласованный механизм определения всех операторов, связанных и не связанных договорными обязательствами с ICANN, которые имеют отношение к регистрации доменных имен в gTLD. В регистрационных записях WHOIS часто не проводится различие между регистраторами и реселлерами. К примеру, при исследовании злоупотребления DNS, выполненном по заказу CCT-RT, не удалось различить реселлеров и регистраторов, чтобы определить, насколько злоупотребления технического характера в DNS со стороны конкретных реселлеров могут влиять на общие объемы злоупотреблений технического характера в DNS. Эти данные необходимо получить, чтобы улучшить сформулированные на основе данных рекомендации CCT-RT, дополнить меры защиты, предусмотренные для программы New gTLD, и повысить качество решений, которые принимает отдел соблюдения договорных обязательств ICANN.

Кому: Правлению ICANN, Группе заинтересованных сторон-регистратур, Группе заинтересованных сторон-регистраторов, Организации поддержки доменов общего пользования, РГ по PDP в отношении последующих процедур, Второй группе по анализу и проверке безопасности, стабильности и отказоустойчивости DNS и Группе по анализу службы каталогов регистрационных данных.
Предварительное условие или уровень приоритета: Высокий
Консенсус в группе: ???

Подробности: Информация WHOIS — важный источник данных при анализе злоупотреблений технического характера в DNS. Такие меры защиты, как требование использовать расширенный вариант записи данных WHOIS, не обязывают указывать реселлеров в регистрационных записях WHOIS. Соответственно, нельзя без труда определить всю цепочку сторон, участвовавших в операции регистрации. Не располагая такой информацией, сложно оценить, насколько злоупотребления технического характера связаны с деятельностью отдельных реселлеров, а не регистраторов. Например, при замалчивании таких данных, реселлер, который причастен к очень большому количеству злоупотреблений, мог бы продолжать работу по договору с регистратором, имеющим относительно нормальный уровень злоупотреблений технического характера. По сути, это позволило бы стороне, не связанной договорными обязательствами, систематически и непрерывно совершать злоупотребления технического характера, несмотря на обязанность соблюдать требования на более низком уровне договорной цепочки. В то время как сбор и опубликование указанных сведений дало бы конечным пользователям возможность без труда определить регистратуру, регистратора и реселлера, связанных с регистрацией доменного имени, чтобы устранить непрозрачность в отношении сторон, отвечающих за сокращение объема злоупотреблений технического характера в DNS. Это позволило бы выполнить более подробный анализ злоупотребления DNS и повысило бы прозрачность для пользователей интернета, тем самым способствуя усилиям сообщества по усовершенствованию подотчетности и контролю со стороны отдела соблюдения договорных обязательств.

6.3 Приложение С. Опросы и исследования

Было поручено провести до начала деятельности группы CCTRT несколько опросов и исследований, результаты которых лягут в основу работы группы:

- В 2013 году Правление ICANN сформировало Консультативную группу по реализации для изучения совокупности возможных показателей, которые были предложены Организацией поддержки доменов общего пользования (GNSO) и Консультативным комитетом At-Large (ALAC). Эта группа — IAG-CCT — оценила возможность практической реализации, полезность и экономическую эффективность нескольких показателей, рекомендованных двумя указанными организациями, и подготовила в общей сложности 66 показателей, утвержденных Правлением ICANN для передачи на рассмотрение CCTRT.¹³⁹ ICANN собирает данные для определения многих из этих показателей.¹⁴⁰ Среди 66 рекомендованных показателей есть несколько таких, в состав которых входят базовые количественные данные, фиксирующие стили поведения и деятельность на рынке доменных имен до появления большого количества новых gTLD. В зависимости от показателя, этот базовый период может охватывать от одного года до нескольких лет, предшествующих делегированию новых gTLD.
 - IAG-CCT пришла к заключению, что наилучшую оценку ряда показателей обеспечивает опрос потребителей и владельцев доменов. Результаты 2-й волны опроса потребителей, проведенного компанией Nielsen, были опубликованы в июне 2016 года.¹⁴¹ В рамках данного исследования измерялось текущее отношение пользователей интернета к пространству gTLD и DNS, а также изменения в настроениях по сравнению с 1-й волной опроса потребителей компанией Nielsen в 2015 году.¹⁴² Интернет-пользователям задавались вопросы о различных аспектах осведомленности пользователей, потребительском выборе, опыте и доверии. Участники опроса потребителей в совокупности сформировали репрезентативную выборку пользователей интернета из всех пяти регионов ICANN. При этом в каждой стране, включенной в состав выборки, опрос проводился на соответствующем государственном языке. Результаты 2-й фазы исследования продемонстрировали, что более половины респондентов (52%) знают о существовании по крайней мере одного нового gTLD и, в целом, доверие к доменной отрасли повысилось, по сравнению с другими высокотехнологичными отраслями.
 - Аналогичным образом компания Nielsen провела глобальный опрос владельцев доменов, целевой группой которого были владельцы хотя бы одного зарегистрированного доменного

¹³⁹ Консультативная группа по реализации поддержки конкуренции, потребительского доверия и потребительского выбора (26 сентября 2014 года), *Итоговые рекомендации по показателям для анализа CCT*, дата просмотра — 20 января 2017 года, <https://community.icann.org/display/IAG/IAG-CCT+report>

¹⁴⁰ ICANN, «Отчетность по показателям конкуренции, потребительского доверия и потребительского выбора (CCT)», дата просмотра — 25 января 2017 года, <https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en>

¹⁴¹ Nielsen, *2-я волна глобального опроса потребителей по поручению ICANN* (июнь 2016 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2-2016-06-23-en>

¹⁴² Nielsen, *Глобальный опрос потребителей по поручению ICANN* (апрель 2015 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2015-05-29-en>

имени. Участникам этого исследования были заданы вопросы, позволяющие оценить осведомленность о новых gTLD и узнать их мнение относительно выбора, взаимодействия и доверия к существующей системе gTLD. Результаты 1-й волны опроса владельцев доменов, проведенного компанией Nielsen, были опубликованы в сентябре 2015 года.¹⁴³ CCTRT получила результаты 2-й волны опроса владельцев доменов 15 сентября 2016 года.¹⁴⁴ Эти результаты показали, что уровни осведомленности о новых gTLD на обоих этапах опроса одинаковые, при этом в Южной Америке и в Азиатско-Тихоокеанском регионе этот показатель выше, а уровень доверия к отрасли в целом, особенно в Азии, остается высоким.

- Вторая подгруппа показателей IAG-CCT предназначена для измерения конкуренции в пространстве новых gTLD на основе анализа данных о ценах и других, не связанных с ценами, индикаторов. ICANN поручила Analysis Group выполнить экономическое исследование с двумя основными целями: сравнить механизмы определения цен на домены в новых gTLD с механизмами, которые используются для существовавших ранее доменов; провести качественный анализ других, не относящихся к ценам, индикаторов конкуренции, таких как технические или иные инновации в сфере бизнеса. Результаты 1-й фазы оценки были представлены Analysis Group в сентябре 2015 года.¹⁴⁵ Во время 2-й фазы оценки Analysis Group определено, как изменились (или не изменились) показатели конкуренции, установленные во время 1-й фазы этой оценки, по мере развития программы New gTLD в течение года.¹⁴⁶ Результаты 2-й фазы экономического исследования, представленные в октябре 2016 года, свидетельствуют о сокращении доли регистраций новых gTLD, принадлежащей четырем и восьми крупнейшим регистраторам, а также об изменчивости долей регистраций, принадлежащих операторам регистратур. Члены CCTRT передали Analysis Group свои комментарии относительно методики и подхода перед началом второго этапа исследования.
- © Чтобы помочь CCTRT определить эффективность процедур приема и оценки заявок в рамках программы New gTLD, а также мер защиты, принятых с целью противодействия злоупотреблениям, ICANN сотрудничала с сообществом для подготовки следующих отчетов:
- Пересмотренный обзор хода реализации программы, опубликованный в январе 2016 года, где рассматривается

¹⁴³ Nielsen, *Глобальный опрос владельцев доменов по поручению ICANN* (сентябрь 2015 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2015-09-25-en>

¹⁴⁴ Nielsen, *2-я волна глобального опроса владельцев доменов по поручению ICANN* (август 2016 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2-2016-09-15-en>

¹⁴⁵ Analysis Group, *Первая фаза исследования оценки воздействия реализации программы New gTLD ICANN на конкуренцию* (сентябрь 2015 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2-2015-09-28-en>

¹⁴⁶ Analysis Group, *Вторая фаза исследования оценки воздействия реализации программы New gTLD ICANN на конкуренцию* (октябрь 2016 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2016-10-11-en>

эффективность и результативность реализации программы New gTLD корпорацией ICANN с точки зрения персонала¹⁴⁷;

- «Пересмотренный отчет: меры защиты от злоупотребления DNS в рамках программы New gTLD», в котором изучены методы оценки эффективности мер, принятых в рамках программы New gTLD для защиты DNS от злоупотреблений. В этом отчете указано, какая деятельность может подходить под определение злоупотребления DNS, и представлен предварительный обзор публикаций о масштабах злоупотреблений в новых gTLD и в DNS в целом¹⁴⁸.
 - «Пересмотренный отчет: анализ механизмов защиты прав, в котором оцениваются важнейшие механизмы защиты, такие как Депозитарий товарных знаков, Служба быстрой приостановки и Процедура разрешения разногласий в отношении товарных знаков после делегирования (PDDRP). Также была рассмотрена взаимосвязь между механизмами защиты прав и другими компонентами программы New gTLD.¹⁴⁹
- ⊙ Чтобы расширить имеющиеся данные, CCTRT предложила провести дополнительные опросы и исследования, результаты которых также лягут в основу работы группы:
- Подгруппа по вопросам конкуренции и потребительского выбора попросила группу по анализу и корпорацию ICANN представить дополнительные данные о ценообразовании и анализе регистраций, способствующие получению в ходе исследования ответов на вопросы о том, насколько эффективно расширение пространства новых gTLD стимулировало ценовую конкуренцию между операторами gTLD, а также между регистраторами и реселлерами.
 - Подгруппа по вопросам конкуренции и потребительского выбора запросила данные о паркинге доменов в существовавших ранее gTLD, чтобы дополнить имеющиеся на веб-сайте ntlidstats.com данные о паркинге в новых gTLD. Эти данные о паркинге позволили подгруппе получить более точное представление о регистрациях в каждой регистратуре, исключив «неактивные» регистрации из общего количества. Помимо этого, подгруппа по вопросам конкуренции и потребительского выбора получила от организаций CENTR и Zooknic данные о регистрациях в ccTLD.
 - По запросу Группы по анализу, ICANN заключила с компанией SIDN договор на проведение исследования для анализа объемов неправомерной, злонамеренной и преступной деятельности в

¹⁴⁷ ICANN, *Обзор хода реализации программы* (январь 2016 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf>

¹⁴⁸ Исследование деятельности и политики ICANN, *Меры защиты от злоупотребления DNS в рамках программы New gTLD: пересмотренный отчет* (июль 2016 года), дата просмотра — 30 января 2017 года, <https://www.icann.org/news/announcement-2016-07-18-en>

¹⁴⁹ ICANN, *Анализ механизмов защиты прав: пересмотренный отчет* (сентябрь 2015 года), дата просмотра — 30 января 2017 года, <https://newgtlds.icann.org/en/reviews/rpm/rpm-review-11sep15-en.pdf>

новых и существовавших ранее gTLD. В отчете «Статистический анализ злоупотреблений DNS в gTLD» сравниваются объемы этой деятельности в существовавших ранее и новых gTLD, а также выполнен дедуктивный статистический анализ для оценки воздействия, которое оказали использование DNSSEC, паркинг доменов и ограничения при регистрации на масштабы злоупотреблений за первые три полных года осуществления программы New gTLD (2014–2016 годы).¹⁵⁰

- На своем третьем очном совещании в июне 2016 года CCTRT попросила организовать проведение опроса кандидатов. Помимо рассмотрения тем, относящихся к конкуренции, потребительскому выбору и доверию, также была поставлена задача оценить в ходе опроса эффективность процедуры приема и оценки заявок в рамках программы New gTLD. CCTRT стремилась получить ответы на указанные вопросы для лучшего понимания мнений о процедуре обработки заявок среди кандидатов, которые успешно прошли эту процедуру, еще проходят ее или отозвали свои заявки.
- Для обоснованного анализа процедуры приема и оценки заявок группа CCTRT обратилась к компании AMGlobal с просьбой провести исследование и взять интервью у представителей компаний, организаций и других учреждений, которые на подавали заявок на новые gTLD, но могли бы считаться хорошими кандидатами на участие в программе, поскольку относятся к той же или аналогичной категории организаций из развитых стран, подавших заявки.¹⁵¹ Цель этого исследования состояла в том, чтобы глубже понять степень осведомленности потребителей о программе New gTLD, а также причины, по которым поступило немного заявок от компаний из развивающихся стран. Отчет был представлен в ноябре 2016 года и содержал, к примеру, рекомендацию создать средства информирования, которые позволят не имеющим специальной подготовки людям получить ясные ответы на важнейшие вопросы о стоимости, процедуре и сроках подачи и рассмотрения заявок, а также о самой ICANN. Также было рекомендовано полностью разъяснить сообществу различные способы применения новых gTLD, отвечая на возможные вопросы сообщества о бизнес-моделях и примерах применения. Что касается будущих раундов приема и оценки заявок, в отчете предлагалось провести дополнительное исследование, чтобы определить наилучшие способы установления контактов с широкой общественностью на глобальном юге и организации диалога на тему новых gTLD в государственном и частном секторах; в максимально возможной степени как можно скорее начать подготовку общественности к следующему раунду.

¹⁵⁰ Лаборатория SIDN и Делфтский технический университет (август 2017 года), *итоговый отчет «Статистический анализ злоупотреблений DNS в gTLD»*, дата просмотра — 23 октября 2017 года, <https://www.icann.org/en/system/files/files/sadaq-final-09aug17-en.pdf>

¹⁵¹ AMGlobal Consulting, «New gTLD и глобальный юг: осмысление причин низкого спроса на домены в последнем раунде программы New gTLD, и оценка вариантов дальнейших действий» («New gTLDs and the Global South: Understanding Limited Global South Demand in the Most Recent New gTLD Round and Options Going Forward»), (октябрь 2016 года), дата просмотра — 25 января 2017 года, <https://community.icann.org/pages/viewpage.action?pageId=56135383>

-
- ⦿ Кроме того, ССТРТ воспользовалась результатами опроса, организованного по заказу Международной ассоциации по товарным знакам (INTA). Во время этого опроса, проведенного в январе-феврале 2017 года, поступила информация от 33 корпоративных членов INTA, корпораций, не входящих в состав INTA, и владельцев прав на интеллектуальную собственность, ответивших на вопросы о расходах, понесенных их клиентами в связи с расширением пространства новых TLD. Этот опрос, анкета которого была разослана 1 096 потенциальным респондентам, позволил изучить практический опыт участия владельцев товарных знаков в этой программе.¹⁵²

¹⁵² Nielsen (апрель 2017 года), опрос INTA для оценки воздействия новых gTLD на расходы, дата просмотра — 24 октября 2017 года, [community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf](https://community.icann.org/download/attachments/56135378/INTA_Cost_Impact_Report_revised_4-13-17_v2.1.pdf)

6.4 Приложение Е. Сводные данные об участии

Имя	Принадлежность	Участие в совещаниях (Общее количество пленарных заседаний и очных совещаний: 65 — по сентябрь 2017 года включительно)
Кэлвин Браун (Calvin Browne)	GNSO	52
Карлос Рауль Гутьеррес (Carlos Raul Gutierrez)	GNSO	46
Карлтон Сэмюэлс (Carlton Samuels)	ALAC	48
Давид Тейлор (David Taylor)	GNSO	47
Деян Джукич (Dejan Djukic)	ccNSO	51
Дрю Бэгли (Drew Bagley)	Независимый эксперт	61
Фабро Стибель (Fabro Steibel)	Независимый эксперт	28
Гао Мосвеу (Gao Mosweu)	ccNSO	49
Джонатан Зук (Jonathan Zuck)	GNSO	55
Джордин Бьюкенен (Jordyn Buchanan)	GNSO	61
Каили Кан (Kaili Kan)	ALAC	59
Лорин Капин (Laureen Kapin)	Представитель председателя GAC	58
Меган Ричардс (Megan Richards)	GAC	48
Н. Рави Шанкер (N.Ravi Shanker) (сложил с себя полномочия 18 октября 2017 года)	Независимый эксперт	2
Стэнли Бесен (Stanley Besen) (сложил с себя полномочия 25 июня 2017 года)	Независимый эксперт	33
Ваудо Сиганга (Waudu Siganga)	GNSO	53
Джейми Хедлунд (Jaime Hedlund)	Представитель президента и генерального директора ICANN	49

Имя	Принадлежность	Подгруппа по вопросам	Подгруппа по вопросам	Заседания подгруппы	Процесс подачи и	Заседания подгруппы
-----	----------------	-----------------------	-----------------------	---------------------	------------------	---------------------

		конкуренции и потребительского выбора (22 заседания по сентябрь 2017 года включительно)	механизмов защиты и доверия (26 заседаний по сентябрь 2017 года включительно)	Nielsen (4 заседания по сентябрь 2017 года включительно)	рассмотрения заявок (3 заседания по сентябрь 2017 года включительно)	INTA (3 заседания по сентябрь 2017 года включительно)
Кэлвин Браун	GNSO	2	14			
Карлос Рауль Гутьеррес	GNSO	5	13	2		0
Карлтон Сэмюэлс	ALAC		17			2
Давид Тейлор	GNSO	1	14			3
Деян Джукич	ccNSO	19			1	2
Дрю Бэгли	Независимый эксперт	2	23		0	
Фабро Стибель	Независимый эксперт		11	3		
Гао Мосвеу	ccNSO		22		1	
Джонатан Зук	GNSO	18	18	3	2	
Джордин Бьюкенен	GNSO	22		3	1	3
Каили Кан	ALAC	16				
Лорин Капин	Представитель председателя GAC		22	2	2	
Меган Ричардс	GAC	12			0	
Н. Рави Шанкер (сложил с себя полномочия 18 октября 2017 года)	Независимый эксперт					
Стейнли Бенсен (сложил с себя полномочия 25 июня 2017 года)	Независимый эксперт	13	1	1		
Ваудо Сиганга	GNSO	16		2	1	1
Джейми Хедлунд	Представитель президента и генерального директора ICANN	6	13		0	

Заявления о заинтересованности членов группы по анализу опубликованы по адресу <https://community.icann.org/display/CCT/Composition+of+Review+Team>.

Архив электронной почты размещен по адресу <https://community.icann.org/display/CCT/Email+Archives>.

