ICANN | GAC
Governmental Advisory Committee

ICANN 65 POLICY FORUM
MARRAKECH
24–27 June 2019

Борьба со злоупотреблениями DNS

Заседание 5.1

Содержание

Цели заседания

- Рассмотреть недавние события и дискуссии в том, что касается определения, обнаружения и борьбы со злоупотреблениями DNS, а также усилий, предпринимаемых для обеспечения соответствия WHOIS требованиям GDPR.
- Обсудить позиции и возможные дальнейшие действия GAC и рабочей группы GAC по обеспечению общественной безопасности (PSWG).

Справочная информация

Злонамеренные действия в Интернете угрожают и оказывают воздействие на владельцев и конечных пользователей доменных имен посредством использования уязвимостей во всех аспектах работы экосистем Интернета и DNS (в протоколах, компьютерных системах, персональных и коммерческих операциях, процессах регистрации доменных имен и т. п.). Некоторые виды такой преступной деятельности угрожают безопасности, стабильности и отказоустойчивости инфраструктуры DNS и всей системы DNS в целом.

В сообществе ICANN такие угрозы и злонамеренные действия обычно называют «злоупотреблениями DNS». Под злоупотреблениями DNS в общем случае понимаются все или некоторые из следующих действий: распределенные атаки типа «отказ в обслуживании» (DDoS), спам, фишинг, вредоносное ПО, ботнеты и распространение противозаконных материалов. При том, что имеется всеобщее согласие в отношении существования проблемы таких злоупотреблений и необходимости ее решения, в отношении того, на кого должна быть возложена ответственность за ее решение, существуют разногласия. В частности, регистратуры и регистраторы озабочены перспективами предъявления к ним дополнительных требований, поскольку это может сказаться на их безнес-модели и прибыльности.

В рамках этой дискуссии необходимо отметить, что споры ведутся даже в отношении точного определения самого термина «злоупотребления DNS»[1].

Тем не менее, за последние годы был достигнут определенный прогресс. Здесь приведена сводка усилий, предпринимавшихся ранее сообществом ICANN для решения проблемы злоупотреблений DNS, причем в некоторых из них с пользой для дела принимал участие GAC:

- В 2008 году **Организация поддержки доменов общего пользования ICANN (GNSO)** сформировала рабочую группу по политике в сфере противодействия злоупотреблениями регистрации. Она определила набор конкретных вопросов, но не представила результаты в виде политики и не обсуждала в дальнейшем необязательные практические рекомендации для регистратур и регистраторов (в т. ч. семинары в рамках конференций ICANN41 и ICANN42).

[1] Свидетельством тому стала дискуссия по теме Злоупотребления DNS и меры защиты потребителей, прошедшая в рамках саммита GDD (7-8 мая 2019 года).

- **В рамках программы New gTLD**[2] корпорация ICANN своим меморандумом о Предотвращении злонамеренного поведения (3 октября 2009 года) утвердила ряд новых требований. Оценка их эффективности была позже изложена в отчете ICANN о механизмах защиты программы New gTLD (18 июля 2016 года) в рамках подготовки к предусмотренной Уставом проверке (проверке конкуренции, потребительского доверия и потребительского выбора).

- До создания рабочей группы GAC по обеспечению общественной безопасности (PSWG) **представители правоохранительных органов** играли ведущую роль в переговорах по соглашению об аккредитации регистраторов в версии от 2013 года[3], а также в выработке рекомендации GAC в отношении угроз безопасности, в результате чего в базовое соглашение об администрировании новых gTLD были включены новые положения, описывающие обязанности регистратур. Позже эти положения были дополнены необязательной концепцией порядка действий операторов регистратур при возникновении угроз безопасности (20 октября 2017 года), которая была согласована **корпорацией ICANN, регистратурами и группой PSWG**.

- **Консультативный комитет по безопасности и стабильности (SSAC)** предоставил сообществу ICANN ряд рекомендаций, в частности, в документах SAC038: канал связи регистратора для борьбы со злоупотреблениями (26 февраля 2009 года) и SAC040: Меры по защите служб регистрации доменов от незаконного использования и злоупотреблений (19 августа 2009 года).

- **Корпорация ICANN** через свою **группу по безопасности, стабильности и отказоустойчивости (SSR)** проводит регулярное обучение сообществ по обеспечению безопасности общественности и содействует в реагировании на масштабные инциденты в области безопасности, в т. ч. в рамках своего ускоренного процесса подачи запросов об обеспечении безопасности регистратур (ERSR). Совсем недавно под руководством **офиса технического директора** ICANN был осуществлен проект платформы отчетности о случаях злоупотребления доменами (DAAR), в рамках которого формируются ежемесячные отчеты о злоупотреблениях. Этот инструмент был активно поддержан как GAC, так и рядом групп по особым проверкам в качестве меры обеспечения транспарентности и определения источников проблем, которые затем могут решаться в рамках обеспечения соблюдения договорных обязательств или, при необходимости, с помощью новых политик.

[2] Тщательные проверки операторов регистратур, требование продемонстрировать план развертывания DNSSEC, запрещение использования символов обобщения имен, удаление осиротевших связующих записей при удалении из файла зоны записи сервера имен, требование поддерживать расширенный вариант записи данных WHOIS, централизация доступа к файлам зон, требование документального оформления контактных данных и политик по вопросам злоупотреблений на уровне регистратур

[3] См. Рекомендации правоохранительных органов в отношении комплексной проверки (октябрь 2019 года) и 12 рекомендаций правоохранительных органов (1 марта 2012 года)

Вопросы

Эти реализованные в прошлом инициативы еще не привели к заметному снижению количества злоупотреблений DNS, скорее, очевидно, что многое еще только предстоит сделать. Несмотря на внимание со стороны сообщества ICANN и существующие отраслевые практические методики по борьбе со злоупотреблениями DNS, действия сообщества под руководством GAC, а также подготовленный по результатам проверки конкуренции, потребительского доверия и потребительского выбора отчет «Статистический анализ злоупотреблений DNS в gTLD» (9 августа 2017 года), в котором подчеркивалась неизменности тенденции к злоупотреблениям, коммерческие практики, способствующие злоупотреблениям, а также свидетельства того, что существуют «возможности для разработки и усовершенствования *существующих мер по борьбе и средств защиты*», а также потенциал для разработки будущих политик[4].

Помимо этого, в результате вступления в силу Общих положений о защите данных (GDPR) Евросоюза и усилий по обеспечению соответствия требованиям системы WHOIS — ключевого инструмента в расследовании преступлений и злоупотреблений — правоохранительные органы, эксперты в области кибербезопасности, специалисты по защита прав потребителей и прав на интеллектуальную собственность высказывают опасения в отношении способности эффективно бороться со злоупотреблениями[5].

В таком контексте консультативные комитеты ICANN, в частности GAC, SSAC и ALAC, а также различные третьи стороны, которых это касается, как сообщает отдел по контролю исполнения договорных обязательств и защиты прав потребителей ICANN, призывают корпорацию ICANN и сообщество ICANN принять дальнейшие меры[6].

Для принятия таких дальнейших мер необходимо, чтобы сообщество ICANN пришло к какого-то рода консенсусу по ряду нерешенных вопросов. Дискуссии о борьбе со злоупотреблениями и потенциальной работе над политиками в сообществе ICANN обычно вращаются вокруг следующих вопросов:

- **Определение злоупотреблений DNS**:
  Что составляет злоупотребление, учитывая круг полномочий ICANN и договора, заключенные корпорацией с регистратурами и регистраторами?

[4]См. комментарий GAC (19 сентября 2017 года) к итоговому отчету «Статистический анализ злоупотреблений DNS в gTLD».

[5]См. разделы III.2 и IV.2 в коммюнике по результатам заседаний GAC на конференции в Барселоне (25 октября 2018 года), в которых приводится ссылка на исследования последствий для правоохранительных органов в разделе 5.3.1 проекта отчета группы проверки службы каталогов регистрационных данных (31 августа 2018 года) и в публикации антифишинговой группы и рабочей группы по борьбе со злоупотреблениями и распространением вредоносного ПО при передаче сообщений и использовании мобильной связи (18 октября 2018 года)

[6]См. материалы дискуссии Злоупотребления DNS и меры защиты потребителей, прошедшей в рамках саммита GDD (7-8 мая 2019 года).

- **Обнаружение и сообщение о злоупотреблениях DNS (с точки зрения осведомленности и прозрачности):**
  Как обеспечить обнаружение злоупотреблений DNS и донесение информации об этом до соответствующих заинтересованных сторон, в т. ч. потребителей и пользователей Интернета?
- **Предотвращение и устранение злоупотреблений DNS (с точки зрения эффективности)**:
  Какие инструменты и процедуры корпорация ICANN, действующие лица и заинтересованные стороны отрасли могут использовать для сокращения количества злоупотреблений и должного реагирования на них? Кто за что отвечает в общей картине и как разные действующие лица могут объединять свои усилия оптимальным способом?

GAC в своих усилиях по повышению безопасности и стабильности ради общего блага пользователей Интернета может решить принять активное участие в продвижении дискуссии по этим вопросам ради достижения прогресса в повышении эффективности предотвращения и устранения злоупотреблений.

Предложение руководства по действиям GAC

В ходе конференции ICANN65 в Марракеше GAC может выполнить следующее:

1. **Призвать к выработке процедуры для прояснения определения злоупотреблений DNS** в том, что касается миссии ICANN и определить свою позицию по этому вопросу. Это помогло бы продвинуться в текущих дискуссиях, которые ведутся в сообществе ICANN в отношении существования такого определения, в а также в отношении рекомендаций группы проверки конкуренции, потребительского доверия и потребительского выбора о злоупотреблениях DNS, рассмотрения этих рекомендаций Правлением ICANN и текущих инициатив отдела защиты прав потребителей ICANN.

2. **Рассмотреть необходимость и возможность разработки политики** в связи с недавним обсуждением такой возможности в ходе саммита GDD[7], отметив при этом позиции, которые GAC занимал по этому вопросу ранее[8].

3. **Рассмотреть действия, предпринятые в отношении рекомендаций группы проверки конкуренции, потребительского доверия и потребительского выбора**, касающихся злоупотреблений DNS (рекомендации 14–19), в т. ч. рассмотрение их Правлением ICANN и работу, порученную Правлением корпорации ICANN, а также дальнейшее рассмотрение их в соответствующих группах интересах и процессах работы ICANN.

4. **Рассмотреть возможность продвижения успешных практических методик в пространстве имен ccTLD,** таких как опыт домена .DK, который был представлен в ходе конференции ICANN64[9], а также применение их в отрасли gTLD.

Связанные темы

Определение злоупотреблений DNS: консенсус в отношении злоупотреблений на уровне инфраструктуры?

Как подчеркивалось в ходе прошедшего недавно саммита GDD (7–9 мая 2019 года), **в сообществе нет широкого согласия в вопросе о том, что составляет «злоупотребление DNS»**, отчасти из-за опасений некоторых заинтересованных сторон в отношении возможного выхода ICANN за пределы мандата корпорации, а также в отношении последствий в том, что касается прав пользователей и прибыльности бизнеса сторон, связанных договорными обязательствами[10].

---

[7] См. материалы дискуссии Злоупотребления DNS и меры защиты потребителей, прошедшей в рамках саммита GDD (7-8 мая 2019 года).

[8] В частности, в своем комментарии (19 сентября 2017 года) к итоговому отчету «Статистический анализ злоупотреблений DNS в gTLD» GAC отметил следующее:

- «*В исследовании злоупотреблений DNS кратко упоминается вывод о том, что определенные URL-адреса чаще других используются для распространения материалов, связанных с насилием над детьми [...] Было бы полезно, если бы в этом отчете подробнее и четче объяснялось это заявление, возможно, с приведением количественных оценок, чтобы заинтересованные стороны могли понять, в какой степени эта проблема была изучена в ходе исследования, а также для использования этой информации в качестве одного из рассматриваемых соображений в ходе возможной разработки политики в будущем*»
- «*Очерченная зависимость между ужесточением правил регистрации имен и сокращением количества злоупотреблений указывает на потенциальные области для разработки политики в будущем».*
- «*использование статистического анализа должно послужить информационной основой для будущих политик, направленных на борьбу со злоупотреблениями DNS, также необходимо провести дополнительный анализ для рассмотрения того, каким образом эта информация может использоваться для поддержки усилий ICANN и ее специалистов по обеспечению безопасности и соблюдения договорных обязательств по реагированию на злоупотребления DNS и повышение эффективности мер по их предотвращению в будущем».*

[9] См. материалы заседания по теме Извлеченные уроки: как домену .DK удалось успешно сократить количество доменных имен, задействованных для злоупотреблений (13 марта 2019 года) и последующее обсуждение его в рабочей группе по обеспечению общественной безопасности (PSWG) (17 апреля 2019 года)

[10] Действительно, определение борьбы со злоупотреблениями может иметь свои последствия в том, что касается круга вопросов, на которые распространяется действие политик и договоров ICANN. Тогда как правительства и другие заинтересованные стороны беспокоятся о последствиях злоупотреблений DNS с точки зрения общественных интересов, в т. ч. общественной безопасности и прав на интеллектуальную собственность, регистратуры и регистраторы беспокоят ограничения на их коммерческую деятельность и конкурентоспособность, а также рост операционных издержек и ответственность за последствия, которые могут затрагивать владельцев доменов в случаях принятия мер к доменам, используемым для осуществления злоупотреблений. Некоммерческие заинтересованные стороны, со своей стороны, обеспокоены нарушением свободы слова и прав владельцев доменов и пользователей Интернета на

При этом, однако, по мнению группы проверки конкуренции, потребительского доверия и потребительского выбора, имеет место **консенсус в отношении того, что представляет собой «нарушение безопасности DNS» или «злоупотребление безопасностью инфраструктуры DNS»**, которое трактуется как «*более технические виды злонамеренных действий»,* такие как вредоносное ПО, фишинг и ботнеты, а также рассылка спама, «*когда он используется как средство доставки для других форм злоупотреблений»* [11].

Недавно **отдел ICANN по контролю исполнения договорных обязательств упомянул «злоупотребления инфраструктурой DNS»** в своем письме о проверках регистратур и регистраторов, когда речь шла о выполнении ими договорных положений соглашения об администрировании новых gTLD (спецификация 11 3b), в котором речь идет об «угрозах безопасности, таких *как фарминг, фишинг, вредоносное ПО и ботнеты*»[12], и соглашения об аккредитации регистраторов (раздел 3.18), в котором речь идет о «*контактных лицах для сообщения о* злоупотреблениях» и о «*сообщении о злоупотреблениях*», при этом конкретное определение понятия «злоупотребления» не приводится, но к нему относится «противозаконная деятельность».

С точки зрения GAC определение «угроз безопасности» в соглашение об администрировании новых gTLD, по сути, в точности повторяет **определение, приведенное в разделе «Проверки безопасности» рекомендации GAC по мерам защиты**, применимым ко всем новым gTLD, из коммюнике GAC по итогам конференции в Пекине (11 апреля 2013 года).

После резолюции Правления от 1 марта 2019 года, которой корпорации ICANN было поручено «*способствовать усилиям сообщества по выработке определения термина «злоупотребление», чтобы создать основу для дальнейших действий по данной рекомендации*»[13], а также усилий отдела защиты прав потребителей корпорации ICANN, **ожидается, что дальнейшее обсуждение определения понятия «злоупотребления» состоится в ходе конференции ICANN66**, которая пройдет в Монреале 2–7 ноября 2019 года.

конфиденциальность, а также разделяют озабоченность сторон, связанных договорными обязательствами, в отношении возможного выхода ICANN за пределы миссии корпорации.

[11] См. стр. 88 в итоговом отчете по результатам проверки конкуренции, потребительского доверия и потребительского выбора (8 сентября 2018 года)

[12] В документе Уведомление относительно Спецификации 11 (3) (b) Соглашения об администрировании нового gTLD (8 июня 2017 года) приводится определение «угроз безопасности», к которым относятся «*фарминг, фишинг, вредоносное ПО, ботнеты и прочие виды угроз безопасности».*

[13] См. стр. 5 оценочного листа в решении Правления в отношении итоговых рекомендаций по результатам проверки конкуренции, потребительского доверия и потребительского выбора

Определение злоупотреблений DNS: диалог о мерах защиты потребителей

С момента расширения круга полномочий отдела ICANN по контролю исполнения договорных обязательств и включения в него функций защиты прав потребителей в 2017 году[14] GAC принял участие в нескольких связанных с этими вопросами инициативах:

- Вступительное слово директора ICANN по мерам защиты потребителей (27 июня 2017 года), в котором обсуждается начало неформальной дискуссии, охватывающей все части сообщества, для повышения осведомленности и углубления понимания в сообществе, а также поиска путей повышения корпорацией ICANN эффективности работы своего отдела по контролю исполнения договорных обязательств и защите прав потребителей.

- Дискуссия в формате вебинара, посвященная соблюдению договорных обязательств и мерам по защите прав потребителей (25 сентября 2017 года), в которой приняли участие почти 100 членов сообщества, в т. ч. обсуждение документа Сводка мер защиты в рамках полномочий ICANN (11 сентября 2017 года), после чего для сбора мнений и предложений сообщества соответствующие вопросы были опубликованы в блоге (11 октября 2017 года):
    - Какую роль должна играть ICANN в сфере борьбы со злоупотреблениями DNS?
    - Существуют ли области в сфере борьбы со злоупотреблениями DNS, на которые не распространяются полномочия ICANN для решения таких проблем?
    - Какие дополнительные инструменты или данные были бы полезны для борьбы со злоупотреблениями DNS?
    - Существуют ли области, в которых были бы полезны какие-либо добровольные меры?
    - Каким образом ICANN должна сотрудничать с другими заинтересованными сторонами в борьбе со злоупотреблениями?
    - Существует ли угроза вмешательства правительств стран в том случае, если сообщество ICANN не сможет удовлетворительным образом решить проблему злоупотреблений DNS?

- Встреча представителей сообществ в Вашингтоне, округ Колумбия, (11 января 2019 года), которая была организована для дальнейшего обсуждения этих вопросов в преддверии возможного в будущем вовлечения в них всего сообщества в рамках конференций ICANN.

[14] При принятии на работу директора по мерам защиты потребителей ICANN (23 мая 2017 года), которому было поручено «повысить информированность о текущих мерах *ICANN, направленных на защиту прав потребителей, содействовать в проведении между заинтересованными сторонами дискуссий, посвященных поиску дополнительных путей повышения ICANN эффективности своих механизмов защиты прав потребителей*»

Совсем недавно, в рамках саммита GDD (9 мая 2019 года), отдел по контролю исполнения договорных обязательств и защите прав потребителей провел заседание, посвященное продолжению текущего диалога:

- **Некоторые стороны, связанные договорными обязательствами, считают свои добровольно принимаемые меры по борьбе со злоупотреблениями адекватными ситуации и возражают против возложения на них новых обязательств**, отчасти из-за ограничений круга полномочий ICANN, а также из-за обременительности, свойственной сообщениям о злоупотреблениях, в отношении которых невозможно принять конкретные меры (зачастую такие сообщения[15] поступают от сторон, не осознающих, что круг возможных мер, которые могут принимать регистратуры и регистраторы, ограничен).
- Другие представители высказали предположение, что **ICANN обязана устанавливать правила и соответствующие поощрительные меры**, направленные на наказание злоумышленников без ущерба для действующих лиц, ответственно относящихся к своим обязанностям (**принцип «платит нарушитель»**), и что **стороны, ответственные за злоупотребления, должны указываться** в соответствующих отчетах ICANN.
- **Корпорация ICANN представила идею процесса разработки политики GNSO** для приведения договоров к соответствию ожиданиям консультативных комитетов и третьих сторон, а также в качестве меры по предотвращению последствий будущих разнородных законодательных норм, которые могут приниматься вместо политик ICANN.
- Это предложение встретило **решительные возражения и призывы к поиску альтернативных путей решения данной проблемы**, в т. ч. путем согласования определений в разных частях сообщества или начала переговоров по соглашению об администрировании доменов верхнего уровня, аналогично тому, как это было сделано для соглашения об аккредитации регистраторов в версии от 2013 года.
- **Стороны, связанные договорными обязательствами**, попросили **корпорацию ICANN оказать содействие в повышении информированности сообщества ICANN** от их имени в ходе конференции ICANN66 в Монреале, в т. ч. провести презентацию, посвященную оптимальным практическим методикам, и предоставить данные, демонстрирующие преобладание сообщений о злоупотреблениях, в отношении которых принятие мер невозможно.

[15] В качестве примера см. раздел *Категории мер, которые могут принимать регистратуры в порядке реагирования на угрозы безопасности* необязательной к исполнению концепции порядка действий операторов регистратур при возникновении угроз безопасности

Информированность и транспарентность: участие сообщества под руководством GAC

GAC и его рабочая группа по обеспечению общественной безопасности (PSWG) за последние несколько лет провели для сообщества в рамках конференций ICANN несколько сквозных мероприятий, **посвященных повышению информированности и поиску решений с участием экспертов в соответствующих областях**, среди которых необходимо отметить:

- В ходе конференции ICANN57 в Хайдарабаде (5 ноября 2016 года) группа PSWG GAC провела заседание по представляющей особый интерес теме Борьба со злоупотреблениями в доменах gTLD, которое прошло в формате обмена мнениями между различными представителями сообщества ICANN. В ходе этого заседания были очерчены следующие вопросы:
  - отсутствие общего понимания того, что собой представляет злоупотребление DNS;
  - разнообразие бизнес-моделей, практик и навыков, обуславливающее различие подходов к борьбе со злоупотреблениями;
  - необходимость более широкого отраслевого сотрудничества, опирающегося на общие данные об угрозах безопасности.

- В ходе конференции ICANN58 в Копенгагене (13 марта 2017 года) группа PSWG GAC выступила модератором сквозного заседания сообщества по теме Поиск эффективных способов борьбы со злоупотреблениями DNS: предотвращение, устранение и реагирование, в ходе которого обсуждались последние тенденции в области борьбы со злоупотреблениями DNS, в частности, с фишингом, а также такие шаблоны поведения регистраторов и регистратур, как частая смена доменных имен, что может потребовать большей координации и более сложных стратегий реагирования от участников отрасли. В ходе этого заседания были также подчеркнуты следующие вопросы:
  - новая инициатива платформа отчетности о случаях злоупотребления доменами (DAAR),
  - текущее сотрудничество между такими отделами корпорации ICANN, как отдел соблюдения договорных обязательств и отдел поддержки безопасности, стабильности и отказоустойчивости, а также
  - возможность использования поступлений от аукционов новых gTLD для финансирования нужд борьбы со злоупотреблениями

- В ходе конференции ICANN60 в Абу-Даби (30 октября 2017 года) группа PSWG организовала и провела сквозное заседание сообщества по теме Отчетность о злоупотреблениях DNS для выработки политик на основе фактов и эффективных мер по борьбе, которое было посвящено поиску путей установления надежных, открытых и эффективных на практике механизмов отчетности о злоупотреблениях DNS для предотвращения и устранения злоупотреблений и выработки политик на основе реальных данных. На этом заседании была подтверждена необходимость опубликования достоверных и подробных данных о злоупотреблениях DNS в составе

данных платформы отчетности о случаях злоупотребления доменами (DAAR). Группа PSWG рассмотрела возможность дальнейшего развития возможных принципов работы GAC[16].

Информированность и транспарентность: исследования злоупотреблений DNS

Ряд мер по защите от злоупотреблений DNS были встроены в программу ввода новых gTLD посредством новых требований,[17] принятых корпорацией ICANN в ее меморандуме о Предотвращении злонамеренного поведения (3 октября 2009 года), а также в рекомендации GAC по средствам защиты в отношении проверок безопасности.

Исходя из оценки корпорацией ICANN эффективности таких механизмов защиты программы New gTLD (18 июля 2016 года), в которой принял участие GAC (20 мая 2016 года), группа проверки конкуренции, потребительского доверия и потребительского выбора призвала провести более всеобъемлющий сравнительный анализ уровня злоупотреблений в новых и старых gTLD, в т. ч. дедуктивный статистический анализ предположений, например, о зависимости уровня злоупотреблений от розничных цен на доменные имена.

Выводы, представленные в отчете «Статистический анализ злоупотреблений DNS в gTLD» (9 августа 2017 года), были вынесены на общественное обсуждение. Предложения сообщества были отражены в отчете (13 октября 2017 года) как конструктивные, была отмечена научная строгость анализа и высказан призыв к проведению дальнейших подобных исследований.

В своих комментариях (19 сентября 2017 года) GAC среди прочих выводов подчеркнул следующее:

- Из данного исследования стало очевидно существование значительных проблем со злоупотреблениями DNS:
    - В некоторых новых gTLD со злоупотреблениями связаны более 50% всех зарегистрированных имен
    - На пять новых gTLD приходится 58,7% доменов в новых gTLD, внесенных в черные списки из-за фишинга
- Существует зависимость между уровнем злоупотреблений и политиками операторов регистратур:
    - наибольшее количество злоупотреблений отмечается по тем регистратурам новых gTLD, операторы которых участвуют в ценовой конкуренции;
    - Злоумышленники предпочитают регистрировать домены в стандартных новых gTLD (открытых для публичной регистрации имен), а не в новых gTLD сообществ (ограничивающих круг лиц, которым разрешена регистрация доменных имен).

[16] См. приложение 1: Принципы борьбы со злоупотреблениями к документу Информационная сводка GAC по борьбе со злоупотреблениями DNS к конференции ICANN60 и отчет по итогам данного заседания, приведенный в коммюнике GAC по итогам конференции в Абу-Даби (p.3)

[17] Тщательные проверки операторов регистратур, требование продемонстрировать план развертывания DNSSEC, запрещение использования символов обобщения имен, удаление осиротевших связующих записей при удалении из файла зоны записи сервера имен, требование поддерживать расширенный вариант записи данных WHOIS, централизация доступа к файлам зон, требование документального оформления контактных данных и политик по вопросам злоупотреблений на уровне регистратур

- Существует потенциал для разработки политик в будущем по следующим аспектам:
    - Последующие раунды ввода новых gTLD в связи с данными, свидетельствующими о том, что степень риска зависит от категории доменов верхнего уровня, в дополнение к строгой политике регистрации
    - Повышение эффективности существующих мер и средств безопасности для борьбы со злоупотреблениями на основе информации такого статистического анализа
- ICANN следует продолжить и расширить использование статистического анализа и данных для измерения и распространения в сообществе информации об уровнях злоупотреблений DNS.

Информированность и транспарентность: платформа отчетности о случаях злоупотребления доменами (DAAR)

Проект корпорации ICANN под названием платформа отчетности о случаях злоупотребления доменами начинался как исследовательский проект, который осуществлялся параллельно участию GAC и группы PSWG в работе Правления и сообщества ICANN, направленной на повышение эффективности борьбы со злоупотреблениями DNS в период между конференциями ICANN57 (ноябрь 2016 года) и ICANN60 (ноябрь 2017 года)[18].

Заявленная цель проекта DAAR — «информирование сообщества ICANN о деятельности, связанной с угрозами безопасности; эти данные сообщество ICANN может затем использовать для принятия информированных решений в области выработки политики и правил». Начиная с января 2018 года для этой цели публикуются ежемесячные отчеты, основанные на объединении регистрационных данных TLD с большим набором надежных показателей репутации и каналов данных об угрозах безопасности[19].

В таком качестве проект DAAR является вкладом в выполнение требования, которое было определено GAC для публикации «*надежных и детализированных данных о злоупотреблениях DNS*» в коммюнике GAC по итогам конференции в Абу-Даби (1 ноября 2017 года). Однако, как отмечается в недавнем письме группы M3AAWG[20] в корпорацию ICANN (5 апреля 2019 года), поскольку информация об угрозах безопасности приводится без классификации по отдельным регистраторам и отдельным доменам верхнего уровня, проект DAAR все еще не оправдывает ожиданий членов группы PSWG GAC и их партнеров в сфере обеспечения кибербезопасности, которые получают из него информацию для практического использования.

[18] См. материалы сквозных заседаний сообщества, которые проводились под руководством группы PSWG GAC в ходе конференций ICANN57 (ноябрь 2016 года), ICANN58 (март 2017 года) и ICANN60 (октябрь 2017 года), а также вопросы к Правлению ICANN об эффективности средств для борьбы со злоупотреблениями DNS в коммюнике GAC по итогам конференции в Хайдарабаде (8 ноября 2016 года), последующие вопросы в коммюнике GAC по итогам конференции в Копенгагене (15 марта 2017 года) и проект ответов (30 мая 2017 года) корпорации ICANN.

[19] Подробнее см. здесь: https://www.icann.org/octo-ssr/daar-faqs

[20] Рабочая группа по вопросам борьбы со злоупотреблениями в сфере обмена сообщениями, вредоносного ПО и мобильной связи

Эффективность. текущие меры безопасности для борьбы со злоупотреблениями DNS в договорах с регистратурами и регистраторами

Основываясь на рекомендациях правоохранительных органов в отношении комплексной проверки (октябрь 2009 года), GAC предложил **включить меры безопасности для борьбы со злоупотреблениями DNS в соглашения ICANN** с регистратурами и регистраторами:

- Соглашение об аккредитации регистраторов в версии от 2013 года (17 сентября 2013 года) было утверждено Правлением ICANN (27 июня 2013 года) после включения положений, в которых учитывались 12 рекомендаций правоохранительных органов (1 марта 2012 года)
- Соглашение об администрировании новых gTLD было утверждено Правлением ICANN (2 июля 2013 года) после включения в него положений, соответствующих рекомендации GAC по средствам защиты, которая была изложена в коммюнике по итогам конференции в Пекине (11 апреля 2013 года), в соответствии с предложением Правления ICANN о реализации мер защиты, предложенных GAC, применительно ко всем новым gTLD (19 июня 2013 года)

После первых нескольких лет работы новых gTLD на конференции ICANN57 в ноябре 2016 года **GAC определил ряд положений и связанных с ними мер защиты, эффективность которых он не смог оценить**. Вследствие этого в коммюнике по итогам конференции в Хайдарабаде (8 ноября 2016 года) GAC попросил Правление ICANN прояснить реализацию этих мер. Это привело к диалогу между GAC и корпорацией ICANN, последующим вопросам, которые были приведены в коммюнике GAC по итогам конференции в Копенгагене (15 марта 2017 года), и проекту ответов (30 мая 2017 года), которые обсуждались в ходе телеконференции между GAC и генеральным директором ICANN (15 июня 2017 года). Ряд вопросов остаются открытыми, были определены также новые вопросы, которые были отражены в последующем рабочем документе (17 июля 2017 года).

Среди открытых тем, представляющих интерес для GAC, следует отметить документ Уведомление относительно Спецификации 11 (3) (b), который был опубликован 8 июня 2017 года в ответ на вопросы некоторых операторов регистратур, которые просили предоставить им указания в отношении обеспечения соблюдения раздела 3b спецификации 11 (3) b соглашения об администрировании новых gTLD. **В этом документе предложен один подход, который операторы регистратур могут добровольно применять** для проведения технического анализа в рамках оценки угроз безопасности и подготовки статистических отчетов, предусмотренных п. 3(b) спецификации 11.

В рамках **регулярных проверок, проводимых отделом по контролю соблюдения договорных обязательств ICANN**, в период с марта по сентябрь 2018 года была проведена целевая проверка *«процессов, процедур и работы инфраструктуры DNS»* 20 gTLD, которая *«продемонстрировала неполноту анализа и отчетов об угрозах безопасности для 13 доменов верхнего уровня (TLD), а также отсутствие каких-либо стандартизированных*

или документированных процедур реагирования на злоупотребления или мер, которые принимались бы в отношении обнаруженных угроз»[21].
Вскоре после этого, в ноябре 2018 года, была начата проверка злоупотреблений на уровне инфраструктуры DNS почти всех gTLD, целью которой было *«обеспечение соблюдения сторонами, связанными договорными обязательствами, своих обязательств согласно договорам в том, что касается злоупотреблений и угроз безопасности на уровне инфраструктуры DNS»*. Как сообщалось в ходе саммита GDD (9 мая 2019 года), корпорация ICANN должна выпустить итоговый отчет по результатам этой проверки (изначально запланированный на май 2019 года) и в настоящее время планирует начать в июле 2019 года аналогичную проверку регистраторов.

Стороны, связанные договорными обязательствами, возражали против таких проверок, считая, что они выходят за рамки их договорных обязательств[22]. Существует понимание того, что группа заинтересованных сторон-регистраторов и группа заинтересованных сторон регистратур **будут работать с отделом по контролю исполнения договорных обязательств корпорации ICANN** над тем, чтобы в итоговом отчете по результатам проверки инфраструктуры DNS регистратур было четко указано, что относится к кругу полномочий ICANN (из опасений того, что это может привести к призывам сообщества начать процесс разработки политики), а также чтобы перед началом проверки регистраторов были приняты во внимание опасения, высказываемые регистраторами.

Эффективность. Необязательная концепция порядка действий операторов регистратур при возникновении угроз безопасности

В рамках программы New gTLD Правление ICANN приняло резолюцию (25 июня 2013 года) включить т. н. «проверки безопасности» из рекомендации GAC по мерам защиты (коммюнике по итогам конференции в Пекине в спецификацию 11 соглашение об администрировании новых gTLD. Однако, поскольку Правление пришло к выводу, что этим положениям недоставало конкретного описания деталей реализации, оно приняло решение пригласить сообщество к участию в разработке рамочной концепции «*порядка действий операторов регистратур при возникновении определенных угроз безопасности, представляющих собой опасность причинения реального вреда (...)*».
В июле 2015 года ICANN сформировала проектную группу из волонтеров из числа представителей регистратур, регистраторов и GAC (в т. ч. членов группы PSWG), которая

[21] Как сообщалось в публикации в блоге от 8 ноября 2018 года, «Соблюдение договорных обязательств: борьба со злоупотреблениями на уровне инфраструктуры DNS»: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

[22] См. письмо группы заинтересованных сторон-регистратур (2 ноября 2019 года) и ответ (8 ноября) на него корпорации ICANN, а также комментарии, опубликованные на странице объявления (15 ноября): регистратуры возражали против вопросов проверки, считая, что угроза принудительного исполнения выходит за пределы их договорных обязательств [в частности согласно п. 3b спецификации 11], и заявляли о своем нежелании «делиться с корпорацией *ICANN и сообществом соответствующей информацией о предпринимаемых нами в настоящее время усилиях по борьбе со злоупотреблениями DNS […] в рамках усилий отдела по контролю исполнения договорных обязательств ICANN, которые выходят за пределы допустимого в соответствии с соглашение об администрировании домена верхнего уровня*»

выработала концепцию порядка действий операторов регистратур при возникновении угроз безопасности и после общественного обсуждения опубликовала ее 20 октября 2017 года.

Данная концепция носит рекомендательный, необязательный характер, в ней описываются возможные ответные действия регистратур при выявлении угроз безопасности, в т. ч. при поступлении сообщений от правоохранительных органов. Ею предусмотрен период времени продолжительностью не более 24 часов для реагирования на высокоприоритетные запросы (непосредственная угроза жизни людей, критически важной инфраструктуре или безопасности детей) из законных и надежных источников, таких как государственные правоохранительные органы или органы защиты общественной безопасности в соответствующей юрисдикции.

В соответствии с рекомендацией 19 группа проверки конкуренции, потребительского доверия и потребительского выбора отложила выполнения задачи по проведению оценки эффективности данной концепции до последующей проверки[23].

Эффективность. профилактические меры и недопущение систематических злоупотреблений

Основываясь на своем анализе сложившейся ситуации в том, что касается злоупотреблений DNS[24], в т. ч. учитывая отчет ICANN о механизмах защиты программы New gTLD (15 марта 2016 года) и независимый статистический анализ злоупотреблений DNS (9 августа 2017 года), группа проверки конкуренции, потребительского доверия и потребительского выбора рекомендовала в отношении злоупотреблений DNS следующее:

- Включить **в соглашения об администрировании доменов верхнего уровня положения, которые побуждали бы принимать профилактические меры для предупреждения злоупотреблений** (рекомендация 14)
- Включить договорные положения, направленные на **недопущение систематического использования тех или иных регистраторов или регистратур** для осуществления злоупотреблений, подрывающих безопасность DNS, в т. ч. определить пороговые значения злоупотреблений, при которых должны автоматически срабатывать запросы обеспечения соблюдения обязательств, а также рассмотреть возможность принятия специальной политики разрешения споров в отношении злоупотреблений DNS (DADRP), если сообщество придет к выводу, что сама корпорация ICANN плохо подходит или неспособна обеспечить выполнение таких положений (рекомендация 15)

[23] Рекомендация 19 группы проверки конкуренции, потребительского доверия и потребительского выбора: *Следующей группе проверки конкуренции, потребительского доверия и потребительского выбора следует рассмотреть «Концепцию порядка действий операторов регистратур при возникновении угроз безопасности» и оценить, является ли эта концепция достаточно понятным и эффективным механизмом сокращения объемов злоупотреблений за счет систематических и конкретных мер реагирования на угрозы безопасности.*

[24] См. раздел 9, «Меры безопасности» (стр. 88) в итоговом отчете по результатам проверки конкуренции, потребительского доверия и потребительского выбора (8 сентября 2018 года).

Правление ICANN приняло решение (1 марта 2019 года) присвоить этим рекомендациям статус «в режиме ожидания» и поручило корпорации ICANN «способствовать усилиям сообщества по выработке определения термина «злоупотребление», чтобы создать основу для дальнейших действий по данной рекомендации».[25]

Текущее положение дел

- Коммюнике GAC по итогам конференции в Найроби (10 марта 2010 года), раздел VI. Рекомендации правоохранительных органов в отношении комплексной проверки
- Коммюнике GAC по итогам конференции в Дакаре (27 октября 2011 года), раздел III. Рекомендации правоохранительных органов
- Коммюнике GAC по итогам конференции в Пекине (11 апреля 2013 года), в частности меры, направленные на проверку безопасности, распространяющиеся на все новые gTLD (стр. 7)
- Коммюнике GAC по итогам конференции в Хайдарабаде (8 ноября 2016 года), в т. ч. рекомендацию по борьбе со злоупотреблениями с запросом ответов на вопросы приложения 1 — Вопросы к Правлению ICANN о борьбе ICANN и сторон, связанных договорными обязательствами, со злоупотреблениями DNS (стр. 14–17)
- Коммюнике GAC по итогам конференции в Копенгагене (15 марта 2017 года), в т. ч. рекомендацию по борьбе со злоупотреблениями с запросом ответов на вопросы оценочного листа GAC в дополнение к приложению 1 к коммюнике GAC по итогам конференции в Хайдарабаде (стр. 11–32)
- Коммюнике GAC по итогам конференции в Барселоне (25 октября 2018 года), в частности разделы III.2 «Рабочая группа GAC по общественной безопасности» (стр. 3) и IV.2 «WHOIS и законодательство о защите данных» (стр. 5)
- Комментарий GAC к первоначальному отчету «Статистический анализ злоупотреблений DNS в gTLD» (SADAG, 21 мая 2016 года)
- Комментарий GAC отчету «Статистический анализ злоупотреблений DNS в gTLD» (SADAG, 19 сентября 2017 года)
- Комментарий GAC к итоговому отчету и рекомендациям по результатам проверки конкуренции, потребительского доверия и потребительского выбора (11 декабря 2018 года)

Основные справочные документы

- Рекомендации правоохранительных органов в отношении комплексной проверки (октябрь 2019 года)
- Рекомендации правоохранительных органов в отношении поправок к соглашению с регистраторами (1 марта 2012 года)

[25] См. стр. 5 оценочного листа в решении Правления в отношении итоговых рекомендаций по результатам проверки конкуренции, потребительского доверия и потребительского выбора

- Рекомендации GAC в отношении мер защиты (проверки безопасности), применимых ко всем новым gTLD (стр. 7) из коммюнике GAC по итогам конференции в Пекине (11 апреля 2013 года)
- Вопросы GAC о борьбе со злоупотреблениями и проект ответов ICANN (30 мая 2017 года) по рекомендациям из коммюнике GAC по итогам конференции в Хайдарабаде (8 ноября 2016 года) и продолжение по этому вопросу в Коммюнике GAC по итогам конференции в Копенгагене (15 марта 2017 года)
- Статистический анализ злоупотреблений DNS в gTLD (9 августа 2017 года)
- Комментарий GAC отчету «Статистический анализ злоупотреблений DNS в gTLD» (SADAG, 19 сентября 2017 года)
- Комментарий GAC (16 января 2018 года) к новым разделам в проекте отчета по результатам проверки конкуренции, потребительского доверия и потребительского выбора (27 ноября 2017 года)
- Итоговый отчет и рекомендации по результатам проверки конкуренции, потребительского доверия и потребительского выбора (8 сентября 2018 года), в частности раздел 9 о мерах защиты (стр. 88)
- Комментарий GAC к итоговому отчету и рекомендациям по результатам проверки конкуренции, потребительского доверия и потребительского выбора (11 декабря 2018 года)
- Правление ICANN Оценочный лист к решению Правления в отношении итоговых рекомендаций по результатами проверки конкуренции, потребительского доверия и потребительского выбора (1 марта 2019 года)

Информация по вопросу

- Заседание GAC 11.1 на конференции ICANN65, посвященное проверкам ICANN (в т. ч. соответствующая информация о положении дел с выполнением рекомендаций по итогам проверки конкуренции, потребительского доверия и потребительского выбора)
- Заседание GAC 8.1 на конференции ICANN65, посвященное WHOIS и политике защиты данных
- Заседание GAC 4.1 на конференции ICANN65, посвященное процессу разработки политики в отношении последующих процедур, применимых к новым gTLD

Описание документа

Совещание	ICANN65, Марракеш, 24-27 июня 2019 года
Название	Борьба со злоупотреблениями DNS
Распространение	Члены GAC и широкая публика (после конференции)
Дата распространения	Версия 1: 6 июня 2019 года