ICANN | GAC
Governmental Advisory Committee

ICANN 71
14–17 June 2021
VIRTUAL POLICY FORUM

Борьба с неправильным использованием DNS

Заседание № 3

Содержание

Для справки 2

Вопросы 3

Предложение руководства по действиям GAC 5

Важные события 9

- Обзор последних событий 9
- Центр внимания: Определение неправильного использования DNS 13
- Центр внимания: Меры безопасности для борьбы с неправильным использованием DNS в договорах с регистратурами и регистраторами 16
- Центр внимания: Необязательная концепция порядка действий операторов регистратур при возникновении угроз безопасности 17
- Центр внимания: Рассмотрение рекомендаций по результатам проверки CCT, касающихся неправильного использования DNS 19
- Центр внимания: Обсуждение разработки политики GNSO по предотвращению неправильного использования DNS 21
- Центр внимания: Отчеты о случаях злоупотребления доменами (DAAR) 22

Текущее положение дел 23

Важнейшие справочные документы 27

Цели заседания

Целью данного заседания является продолжение рассмотрения комитетом GAC инициатив ICANN и сообщества ICANN по предотвращению и смягчению последствий неправильного использования DNS, в том числе в ответ на рекомендации по результатам проверок CCT и SSR2 и дискуссии после подготовки итогового отчета РГ по PDP GNSO, которая занималась разработкой последующих процедур, применимых к новым gTLD. На этом заседании также будет продолжено обсуждение возможных конкретных предложений GAC по данному вопросу.

Для справки

Злонамеренные действия в Интернете угрожают и оказывают воздействие на владельцев и конечных пользователей доменов 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.). Такая деятельность угрожает безопасности, стабильности и отказоустойчивости инфраструктуры DNS и всей системы DNS в целом.

В сообществе ICANN такие угрозы и злонамеренные действия обычно называют «неправильным использованием DNS». Под неправильным использованием DNS обычно подразумеваются все или некоторые из следующих действий: фишинг, вредоносное ПО, ботнеты, распределенные атаки типа «отказ в обслуживании» (DDoS), спам и распространение противозаконных материалов. Однако необходимо отметить, что споры ведутся даже в отношении точного определения самого термина «неправильное использование DNS».

Хотя в целом заинтересованные стороны в сообществе ICANN, похоже, согласны с тем, что неправильное использование DNS является проблемой и требует решения, мнения о степени ответственности соответствующих сторон расходятся. Например, регистратуры и регистраторы озабочены возможностью появления у них новых договорных обязательств (которые могут повлиять на их бизнес-модели) и утверждают, что их инструменты противодействия неправильному использованию ограничены и могут оказаться неприемлемыми (для устранения некоторых видов неправильного использования требуется принятие мер хостинг-провайдерами, а некоторые действия регистратуры или регистратора могут привести к сопутствующему ущербу и потенциальной ответственности).

Известные усилия сообщества ICANN по борьбе с неправильным использованием DNS на сегодняшний день имели разную степень успеха:

- В 2008 году **Организация поддержки доменов общего пользования ICANN (GNSO)** сформировала рабочую группу по политике борьбы со злоупотреблениями при 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 том числе на семинарах в рамках конференций ICANN41 и ICANN42).
- **В рамках программы New gTLD,** корпорация ICANN утвердила ряд новых требований[1] своим меморандумом о предотвращении злонамеренного поведения (3 октября 2009 года). 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 конкуренции, потребительского выбора и потребительского доверия (CCT), рекомендации которой были представлены 8 сентября 2018 года.

[1] Тщательные проверки операторов регистратур, требование продемонстрировать план развертывания DNSSEC, запрет на использование символов обобщения имен, удаление «осиротевших» связующих записей при удалении из файла зоны записи DNS-сервера, требование поддерживать расширенный вариант записи данных WHOIS, централизация доступа к файлам зон, требование документировать контактные данные и процедуры в области злоупотреблений на уровне регистратур

- До создания рабочей группы GAC по обеспечению общественной безопасности (PSWG) **представители правоохранительных органов** играли ведущую роль в **переговорах по соглашению об аккредитации регистраторов в редакции от 2013 года**[2], а также в выработке рекомендаций GAC в отношении угроз безопасности, в результате чего в базовое соглашение об администрировании новых gTLD были включены новые положения, описывающие обязанности регистратур[3].

- **Позднее офис CTO корпорации ICANN,** разработал платформу отчетности о случаях злоупотребления доменами (DAAR), которая поддерживает ежемесячные отчеты о жалобах на неправильное использование и отслеживает тенденции, как недавно сообщалось GAC (24 февраля 2021 года). Отслеживание и отчетность о неправильном использовании DNS активно поддерживаются как GAC, так и группами по анализу, которые рекомендовали внести усовершенствования. Ожидается, что такие инструменты создадут транспарентность и помогут определить источники проблем, которые затем могут решаться в рамках обеспечения соблюдения договорных обязательств или, при необходимости, с помощью новой политики.

Вопросы

Реализованные в прошлом инициативы еще не привели к заметному снижению неправильного использования DNS, скорее, очевидно, что многое еще только предстоит сделать. Несмотря на внимание со стороны сообщества ICANN и существование передовой отраслевой практики борьбы с неправильным использованием DNS, действия сообщества под руководством GAC, а также групп по анализу подчеркнули сохранение тенденций совершения злоупотреблений и коммерческой практики, способствующей неправильному использованию, а также позволили получить доказательства того, что имеются «*возможности для разработки и усовершенствования существующих мер по борьбе и средств защиты*», а также потенциал для будущей выработки политики[4].

Помимо этого, правоохранительные органы, эксперты в области кибербезопасности, специалисты по защите прав потребителей и прав на интеллектуальную собственность[5] высказывают опасения в отношении способности бороться с неправильным использованием DNS в результате вступления в силу Общих положений о защите данных (GDPR) Евросоюза и осуществления мероприятий по изменению системы WHOIS — ключевого инструмента в

---

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

[3] Позже эти положения были дополнены не имеющей обязательной силы Концепцией порядка действий операторов регистратур при возникновении угроз безопасности (20 октября 2017 года), которая была согласована корпорацией ICANN, регистратурами и группой PSWG GAC.

[4] См. комментарий GAC (19 сентября 2017 года) к итоговому отчету «Статистический анализ неправильного использования 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), где упоминаются исследования последствий для правоохранительных органов, указанные в разделе 5.3.1 проекта отчета группы по анализу RDS (31 августа 2018 года) и в публикации антифишинговой рабочей группы и рабочей группы по борьбе со злоупотреблением рассылкой сообщений (18 октября 2018 года)

расследовании преступлений и злоупотреблений — с целью обеспечить соответствие требованиям GDPR. Совсем недавно глобальная чрезвычайная ситуация в области здравоохранения, связанная с COVID-19, стала иллюстрацией существующих проблем в связи с резким увеличением объемов регистрации доменов, имеющих отношение к пандемии.

Консультативные комитеты ICANN, в частности GAC, SSAC и ALAC, а также различные третьи стороны, которых это касается, 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?
- **Обнаружение случаев неправильного использования DNS и информирование о таких случаях:** Как обеспечить обнаружение неправильного использования DNS и донесение информации об этом до соответствующих заинтересованных сторон, в том числе потребителей и интернет-пользователей?
- **Предотвращение и смягчение последствий неправильного использования DNS**: 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.

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

Предложение руководства по действиям GAC

1. **Рассмотреть отчет рабочей группы SSAC по вопросам неправильного использования DNS**, в котором предлагается основанный на функциональной совместимости подход к борьбе со злоупотреблениями в DNS (19 марта 2021 года) с целью оценки, в частности, предложения создать «Единого координатора реагирования на злоупотребления» как полностью независимую, неправительственную некоммерческую организацию, которая будет выступать в качестве посредника для всей экосистемы DNS, в том числе для сторон, связанных договорными обязательствами с ICANN, хостинг-провайдеров, интернет-провайдеров (ISP) и сетей доставки контента (CDN), чтобы оптимизировать систему информирования о неправильном использовании и свести к минимуму виктимизацию от злоупотреблений.

2. **Рассмотреть текущие результаты обсуждения GNSO неправильного использования DNS** в свете «дискуссий между Советом GNSO и GAC во время ICANN70» и ранее выраженной серьезной озабоченности GAC по поводу решения Рабочей группы GNSO по процессу разработки политики в отношении последующих процедур, применимых к новым gTLD, не давать никаких рекомендации в этой области.

3. **Обсудить возможные следующие шаги,** в том числе подготовку **конкретных предложений по улучшению политики и (или) положений договоров и контроля за их соблюдением**[7] для решения вопросов государственной политики, связанных с неправильным использованием DNS, которые выявлены в рамках различных усилий сообщества и указаны в комментариях GAC:

    a. **Рекомендации по результатам проверки CCT** в соответствии с ее итоговым отчетом (8 сентября 2018 года), учитывая:

        – Решение Правления ICANN (1 марта 2019 года) по всем 35 рекомендациям, последующее утверждение (26 января 2020 года) предложенного плана выполнения 6 принятых рекомендаций (6 сентября 2019 года) и последнюю резолюцию Правления ICANN (22 октября 2020 года) с описанием действий по 11 из 17 первоначально отложенных рекомендаций, принятую на основании результатов подробной оценки, которую выполнила корпорация ICANN;

        – Вклад GAC в комментарии к проекту отчета (19 мая 2017 года), комментарии к документуСтатистический анализ неправильного использования DNS в gTLD (19 сентября 2017 года), комментарии к дополнительным проектам рекомендаций (15 января 2018 года), комментарии к итоговому отчету по

[7] В соответствии с Коммюнике по результатам заседаний GAC на конференции ICANN69, раздел IV.2: *«GAC считает, что на данный момент есть твердая и широкая поддержка конкретных действий, которые необходимо предпринять для решения отдельных вопросов эффективного устранения неправильного использования DNS»;* протокол совещания GAC на конференции ICANN69: раздел 2.2 *«Пункты программы действий: PSWG GAC должна рассмотреть возможность разработки конкретного предложения, касающегося шагов по борьбе с неправильным использованием DNS, чтобы подготовить GAC к дальнейшему обсуждению этого вопроса на конференции ICANN70 (согласно результатам заключительного заседания GAC)».*

анализу CCT (11 декабря 2018 года), комментарии к плану выполнения рекомендаций (21 октября 2019 года);

- Рекомендации GAC в Коммюнике по результатам заседаний GAC на конференции в Монреале (6 ноября 2019 года) *не приступать к новому раунду создания gTLD до полного выполнения рекомендаций из отчета группы по анализу конкуренции, потребительского доверия и потребительского выбора, которые были определены в качестве «предварительных условий» или имеют «высокий приоритет»*
- Уточняющие вопросы Правления (16 декабря 2019 года) относительно рекомендаций GAC, подготовленных на конференции в Монреале, включая вопросы, касающиеся проверки CCT, последующих раундов программы New gTLD и определения понятия «полное выполнение»
- Ответ GAC на уточняющие вопросы Правления (22 января 2020 года)
- Ответ Правления на ответ GAC на уточняющие вопросы (11 февраля 2020 года), касающиеся его решения (26 января 2020 года) не принимать и не отклонять рекомендации.

b. Рекомендации группы по анализу безопасности, стабильности и отказоустойчивости (SSR2), представленные в ее итоговом отчете (25 января 2021 года), которые GAC прокомментировал (8 апреля 2021 года)и которые Правление ICANN планирует официально рассмотреть до 25 июля 2021 года.

c. Рабочая группа GNSO по процессу разработки политики в отношении последующих процедур, применимых к новым gTLD, которая указала в своем итоговом отчете (1 февраля 2021 года), что «*эта Рабочая группа по PDP не дает никаких рекомендаций в отношении борьбы с неправомерным использованием доменных имен, за исключением заявления о том, что любые такие будущие усилия должны охватывать как существующие, так и новые gTLD (а, возможно, и ccTLD)»,* несмотря на соответствующие рекомендации, касающиеся неправильного использования DNS, адресованные ей группой по анализу CCT[8]. GAC выразил серьезную озабоченность по поводу этого решения в Комментариях GAC (29 сентября 2020 года) к проекту итогового отчета этой Рабочей группы по PDP и заявил о том, что ожидает от Совета GNSO принятия незамедлительных мер по этому вопросу.

d. Реализация и контроль исполнения основных договорных обязательств в соглашениях с регистратурами и регистраторами, в частности:

- **Спецификация 11 соглашения об администрировании нового gTLD** и соответствующие рекомендации GAC по мерам защиты в Коммюнике по результатам заседаний GAC в Пекине (11 апреля 2013 года), учитывая выводы аудита мер по устранению угроз безопасности DNS, принимаемых

[8] См. итоговый отчет рабочей группы по PDP Sub Pro, Рекомендация № 9.15 (стр. 42) и соответствующее решение Правления ICANN по рекомендациям CCT.

операторами регистратур (17 сентября 2019 года), и обсуждение на встрече GAC и ICANN в формате «вопрос-ответ» (30 мая 2017 года), в Комментариях GAC к проекту отчета CCT (19 мая 2017 года) и в Комментариях GAC к проекту отчета SSR2 (3 апреля 2020 года)

- **Спецификация программы обеспечения точности данных WHOIS** соглашения об аккредитации регистраторов в редакции от 2013 года, которая содержит положения о проверке, подтверждении и точности регистрационных данных домена, как описано в Комментариях GAC к итоговому отчету о проверке RDS-WHOIS2 (23 декабря 2019 года), и раздел **Канал связи с регистратором для борьбы со злоупотреблениями и обязанность расследовать сообщения о злоупотреблениях** (раздел 3.18), требования которого в настоящее время являются предметом начавшейся аудиторской проверки соблюдения договорных обязательств в отношении 153 выбранных регистраторов (15 января 2021 года). Обе эти темы также обсуждались на встрече GAC и ICANN в формате «вопрос-ответ» (30 мая 2017 года) после получения рекомендаций GAC в Коммюнике по результатам заседаний в Хайдарабаде (8 ноября 2016 года)

e. **Обсуждение сообществом неправильного использования DNS и эффективности соответствующих положений договоров**, как с точки зрения контроля за соблюдением, так и исковой силы:

- **Заседания на конференциях ICANN**: вебинар перед началом ICANN66 (15 октября 2019 года), заседание At-Large на ICANN66 по вопросам, волнующим конечных пользователей (3 ноября 2019 года), заседание сквозной группы сообщества на ICANN66, посвященное вопросам неправильного использования DNS (6 ноября 2019 года), заседание At-Large на ICANN67 по вопросам соблюдения договорных обязательств (9 марта 2020 года), заседание ALAC на ICANN68, посвященное обязательствам по обеспечению общественных интересов и соответствующей процедуре разрешения споров (22 июня 2020 года), заседание Совета GNSO и Правления на ICANN68, на котором обсуждались возможные очередные шаги в отношении неправильного использования DNS (14 июня 2020 года), и пленарное заседание на ICANN69 по вопросам неправильного использования DNS (20 октября 2020 года)
- **Переписка Правления ICANN с группой интересов коммерческих пользователей и группой интересов по вопросам интеллектуальной собственности** GNSO, в том числе: Заявление BC относительно обсуждения в сообществе неправильного использования DNS (28 октября 2019 года),письмо BC Правлению ICANN (9 декабря 2019 года), и последующий ответ (12 февраля 2020 года), за которым последовало письмо IPC Правлению ICANN (24 апреля 2020 года)

f. **Реализация используемых операторами ccTLD для борьбы со злоупотреблениями профилактических мер**, которые могли создать основу для совершенствования

практической деятельности регистратур gTLD, например таких мер, которые были представлены ccTLD .EU и .DK[9]

g. **Рекомендации группы по анализу RDS-WHOIS2**, подробно изложенные в ее итоговом отчете (8 октября 2019 года), которые имеют отношение к законному использованию WHOIS в качестве основного инструмента расследования преступлений и злоупотреблений, учитывая Комментарии GAC (23 декабря 2019 года) ирешения Правления ICANN на сегодняшний день (25 февраля 2020 года)

4. **Рассмотрение и дальнейшее отслеживание прогресса в основных усилиях сообщества ICANN по противодействию неправильному использованию DNS** для создания информационной основы и продвижения повышенных стандартов в практической деятельности и договорах:

   a. **Реализация добровольных мер регистраторами и регистратурами gTLD** согласно отраслевой концепции борьбы со злоупотреблениями, и продолжающееся обсуждение в рамках политической сети «Интернет и юрисдикция»[10]

   b. **Усовершенствования платформы отчетности о случаях злоупотребления доменами (DAAR) ICANN,** ранее обсуждавшиеся регистраторами, GAC и SSAC, а также офисом технического директора ICANN[11]

   c. 27 марта 2020 года корпорация ICANN внеслапоправку в соглашение об администрировании домена верхнего уровня .COM, которая **расширяет действие договорных положений, способствующих обнаружению случаев неправильного использования DNS и информированию о них** (включая раздел 3b спецификации 11), **охватывая две трети пространства имен gTLD** (до настоящего момента они применялись только к новым gTLD). Кроме того, в имеющем юридическую силу протоколе о намерениях, подписанном корпорацией ICANN и Verisign, определена концепция сотрудничества в области определения передовых методов и возможных новых договорных обязательств, а также мер, направленных на оценку и смягчение угроз безопасности DNS.

---

9 См., в частности, презентацию EURid (28 января 2016 года) и презентацию .DK во время ICANN64 (12 марта 2018 года)

10 Участники политической сети «Интернет и юрисдикция» недавно (22 февраля 2021 года) объявили о внедрении набора инструментов «Действия на уровне DNS по борьбе с неправильным использованием», который планируют представить 18 марта на конференции.

11 См. последний отчет рабочей группы RySG по DAAR (9 сентября 2020 года), ответ технического директора ICANN (30 сентября 2020 года) и актуальную информацию OCTO для GAC (24 февраля 2021 года)

Важные события

Обзор последних событий

- **На последних конференциях ICANN** руководители PSWG GAC провели подробные брифинги для GAC по проблеме неправильного использования DNS (см. информационные материалы заседаний GAC на ICANN66 и ICANN68, брифинг для GAC на ICANN68 по проблеме неправильного использования DNS, а также отчет PSWG перед GAC на ICANN69 изаседание на ICANN70).
    - GAC рассмотрел доступные регистратурам и регистраторам меры по предотвращению неправильного использования DNS, в частности роль политики регистрации (включая проверку личности) и стратегий ценообразования как ключевых факторов, определяющих количество злоупотреблений в конкретном TLD.
    - GAC также рассмотрел текущие и возможные инициативы по повышению эффективности борьбы с неправильным использованием DNS на уровне Правления ICANN и корпорации ICANN (см. протоколы ICANN66, Коммюнике по результатам заседаний GAC на ICANN68 и соответствующие протоколы, Коммюнике по результатам заседаний GAC на ICANN69 и соответствующие протоколы и Коммюнике по результатам заседаний GAC на ICANN70 и соответствующие протоколы).
    - План работы PSWG на 2020–2021 годы охватывает все эти области в рамках Стратегической цели №1 «Развитие возможностей по сокращению неправильного использования DNS и киберпреступности».
- **Рекомендации по результатам проверки SSR2**
    - Группа по анализу SSR2 представила Проект отчета (24 января 2020 года), в котором делается акцент на мерах по предотвращению и смягчению последствий неправильного использования DNS. Комментарий GAC (3 апреля 2020 г.) одобрил многие рекомендации, в частности те, которые касаются улучшения платформы отчетности о случаях злоупотребления доменами (DAAR) и укрепления механизмов соблюдения требований.
    - Итоговый отчет (25 января 2021 года) был рассмотрен GAC на конференции ICANN70 при подготовке к отправке окончательных комментариев GAC (8 апреля 2021) в рамках общественного обсуждения.
    - Ожидается, что Правление ICANN официально рассмотрит итоговый отчет проверки SSR2 до 25 июля 2021 года в соответствии с шестимесячным сроком, установленным Уставом ICANN.
- **Рабочая группа по борьбе с неправильным использованием DNS Консультативного комитета по безопасности и стабильности (SSAC)** представила свой отчет, опубликованный как документ SAC115 (19 марта 2021 года), в котором предлагается основанный на функциональной совместимости подход к решению проблемы со злоупотреблениями в DNS.

- На конференции ICANN66 SSAC сообщил PSWG о создании Рабочей группы по борьбе с неправильным использованием DNS, в работе которой **принял участие один из сопредседателей PSWG GAC**.
- В указанном отчете **SSAC предложил общую концепцию передовых методов и процессов** для оптимизации отчетности о неправильном использовании DNS и злоупотреблениях в интернете в целом. В частности, там рассмотрены следующие вопросы: Основной центр ответственности за устранение злоупотреблений, стандарты доказывания, каналы передачи разрешения проблем на более высокий уровень, разумные сроки принятия мер, а также доступность и качество контактной информации.
- **Основное предложение**, которое SSAC рекомендует сообществу ICANN изучить и доработать в сотрудничестве с широким сообществом инфраструктуры DNS: **создать «Единого координатора реагирования на злоупотребления»** как полностью независимую, неправительственную некоммерческую организацию, которая будет выступать в качестве посредника для всей экосистемы DNS, в том числе для сторон, связанных договорными обязательствами с ICANN, хостинг-провайдеров, интернет-провайдеров (ISP) и сетей доставки контента (CDN), чтобы оптимизировать систему информирования о неправильном использовании и свести к минимуму виктимизацию от злоупотреблений.

- **Меры и инициативы регистратур и регистраторов по борьбе с неправильным использованием DNS**
  - 27 марта 2020 года корпорация ICANN внеслапоправку в соглашение об администрировании домена верхнего уровня .COM, которая **расширяет действие договорных положений, способствующих обнаружению случаев неправильного использования DNS и информированию о них** (включая раздел 3b спецификации 11), **охватывая две трети пространства имен gTLD положения** (до настоящего момента они применялись только к новым gTLD). Кроме того, в имеющем юридическую силу протоколе о намерениях, подписанном корпорацией ICANN и Verisign, определена концепция сотрудничества в области определения передовых методов и возможных новых договорных обязательств, а также мер, направленных на оценку и смягчение угроз безопасности DNS.
  - **В контексте кризиса COVID-19 стороны, связанные договорными обязательствами, рассказали о своих действиях и извлеченных уроках** до начала и в ходе конференции ICANN68, а заинтересованные стороны PSWG сообщили о текущей совместной работе со странами-членами ЕС, Европолом, ccTLD и регистраторами, направленной на облегчение подготовки отчетов, их рассмотрение и передачу их в соответствующие юрисдикции путем принятия стандартизированной формы для сообщения о домене/контенте, связанным с COVID-19, и создания единого контактного центра для соответствующих органов. Эти усилия основываются на рабочих отношениях, установленных между правоохранительными органами и регистраторами, а также на публикации **Группой заинтересованных сторон-**

регистраторов документа Порядок обращения к регистратору с жалобами на неправомерное использование доменов, о котором сообщалось на ICANN67.

- **Регистратура доменов общественного характера (PIR)**, оператор регистратуры .ORG и несколько новых gTLD сформировали (17 февраля 2021 года) **Институт по борьбе с неправильным использованием DNS**, заявленная цель которого: «*собрать вместе лидеров в области борьбы со злоупотреблениями, чтобы: финансировать исследования, публиковать рекомендуемые методы работы, обмениваться данными и предоставлять инструменты для выявления случаев неправильного использования DNS и информирования о них*». Эта инициатива была представлена группе PSWG GAC (3 марта 2021 года) в преддверии вебинара, который состоится 16 марта 2021 года в Институте по борьбе с неправильным использованием DNS.
  В своем Коммюнике по результатам заседаний на ICANN70 GAC приветствовал создание Института по борьбе с неправильным использованием DNS и «*приз[вал] сообщество объединить усилия для принятия комплексных мер, направленных на решение проблемы неправильного использования DNS*».

- **Комплексный подход корпорации ICANN к реагированию и обеспечение исполнения договорных обязательств**
  - 20 апреля 2020 года Генеральный директор ICANN опубликовал в блоге статью Комплексный подход корпорации ICANN к реагированию на неправильное использование DNS
  - **Офис технического директора ICANN (OCTO) и его группа по обеспечению стабильности и отказоустойчивости** (SSR) проводят исследования и поддерживают опыт ICANN в области безопасности DNS на благо сообщества. Он участвует в различных форумах по разведке киберугроз и реагированию на инциденты, включая Форум групп быстрого реагирования и отделов безопасности (FIRST), рабочую группу по борьбе со злоупотреблением рассылкой сообщений (M3AAWG), Антифишинговую рабочую группу (APWG), американский Национальный альянс киберэкспертизы и обучения (NCFTA) и недавние Коалицию по противодействию угрозам, связанным с COVID-19 (CTC), и Лигу анализа киберугроз, связанных с темой COVID-19 (CTI).
    Он также разрабатывает системы и инструменты для помощи в выявлении, анализе и предоставлении отчетности о неправильном использовании DNS:
    - В ответ на кризис COVID-19 OCTO разработал инструмент **Сбор информации и отчетность по угрозам безопасности доменных имен (DNSTICR)**, помогающий идентифицировать доменные имена, используемые для злоупотреблений, связанных с COVID-19, и делиться данными с соответствующими сторонами. GAC был проинформирован по этому вопросу перед началом ICANN68 (12 июня 2020 г.), а сообщество ICANN – в ходе конференции ICANN68.
    - Через свою **Платформа отчетности о случаях неправильного использования доменов (DAAR)** ICANN осуществляет ежемесячные публикации с января 2018 года о регистрации доменных имен и угрозах безопасности, наблюдаемых в DNS. Она также отслеживает тенденции с помощью

индикаторов работоспособности технологий идентификаторов (ITHI). Некоторые заинтересованные стороны и участники инициатив ICANN прокомментировали ограничения DAAR, в частности в письме M3AAWG в корпорацию ICANN (5 апреля 2019 года) и в Проекте отчета группы по анализу SSR2 (24 января 2020 года). GAC поддержал эти комментарии (см. ниже). Группа заинтересованных сторон-регистратур, которая также выразила свою озабоченность по поводу платформы DAAR и сотрудничает с ICANN в деле ее развития, недавно представила рекомендации в письме техническому директору ICANN (9 сентября 2020 года).

- ICANN OCTO также поддерживает недавно организованную (6 мая 2020 года) **Техническую группу по развитию инициативы по координации деятельности в области безопасности и защиты DNS**, которая была создана в рамках реализации Стратегического плана на 2021-2025 ФГ для *«изучения идей относительно того, что ICANN может и должна делать для повышения уровня сотрудничества и взаимодействия с заинтересованными сторонами в экосистеме DNS для укрепления безопасности DNS»*. Рекомендации ожидаются к маю 2021 года.
- Во время телеконференции GAC по вопросам неправильного использования DNS (24 февраля 2021 года) **корпорация ICANN предоставила обновленную информацию о деятельности OCTO, связанной с неправильным использованием DNS**, в том числе состоялось обсуждение определения понятий «угроза безопасности DNS» и «неправильное использование DNS», обязательств договорных сторон, платформы отчетности о случаях злоупотребления доменами (DAAR), платформы сбора информации и предоставления отчетности об угрозах безопасности доменных имен (DNSTICR), состояния дел с инициативой по вопросам обеспечения безопасности системы доменных имен (DSFI), новой инициативы по обмену знаниями и установлению норм безопасности доменных имен (KINDNS), а также анализ усилий OCTO в области обучения и наращивания потенциала во всем мире.
- **Обеспечение соблюдения договорных обязательств**: в своем блоге (20 апреля 2020 года) генеральный директор ICANN напомнил следующее: «*Отдел соблюдения договорных обязательств ICANN обеспечивает соблюдение обязательств, предусмотренных политиками и соглашениями ICANN, в т. ч. соглашением об администрировании домена верхнего уровня (RA) и соглашением об аккредитации регистраторов (RAA). Кроме того, этот отдел ICANN в тесном сотрудничестве с OCTO занимается выявлением угроз безопасности DNS [...] и определением сторон, связанных договорными обязательствами, которые поддерживают эту деятельность. С помощью данных, собираемых при проведении аудита [...], отдел ICANN по контролю исполнения договорных обязательств оценивает степень соблюдения регистратурами и регистраторами своих обязательств в части борьбы с угрозами безопасности DNS. Помимо данных, получаемых в процессе аудита, отдел ICANN по контролю исполнения договорных обязательств использует данные, собранные OCTO и другими сторонами, для профилактической работы с регистратурами и регистраторами,*

ответственными за непропорционально большое количество угроз безопасности DNS. Если конструктивное сотрудничество не приносит результата, отдел по контролю исполнения договорных обязательств ICANN готов принимать принудительные меры против тех, кто отказывается добровольно исполнять свои обязательств, связанные с угрозами безопасности DNS». Эта заметка в блоге также дает представление об объемах жалоб, ресурсах, выделенных на их обработку, и статистике по разрешению этих жалоб.

Центр внимания: Определение неправильного использования DNS

Как подчеркивалось в ходе саммита GDD (7–9 мая 2019 года), **в сообществе нет широкого согласия в вопросе о том, что составляет «неправильное использование 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.[12]

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».*[13]

Отдел ICANN по контролю исполнения договорных обязательств упоминал о «неправильном использовании инфраструктуры DNS» и «угрозах безопасности» в своем письме о проверках регистратур и регистраторов, рассматривая выполнение 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*»[14], и соглашения об аккредитации регистраторов (раздел 3.18), в котором речь идет о «*контактных лицах для информирования о неправильном использовании*», а также о «*сообщениях о неправильном использовании*». При этом конкретное определение

---

[12] 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 неправильного использования 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 интернет-пользователей на конфиденциальность, а также разделяют озабоченность сторон, связанных договорными обязательствами, в отношении возможного выхода ICANN за пределы миссии корпорации.

[13] См. стр. 88 в итоговом отчете по результатам проверки конкуренции, потребительского доверия и потребительского выбора (8 сентября 2018 г.), как было отмечено недавно в Заявлении GAC о неправильном использовании DNS (18 сентября 2019 г.)

[14] В документе «Уведомление относительно раздела 3b спецификации 11 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».*

понятия «неправильное использование» не приводится, но к нему относится «противозаконная деятельность».

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

Во время вебинара перед ICANN66 15 октября 2019 года **PSWG и стороны, связанные договорными обязательствами, обсудили текущие вопросы и отраслевую практику**. В рамках подготовки к этому вебинару Группа заинтересованных сторон-регистратур опубликовала открытое письмо (19 августа 2019 года), в котором обсуждаются взгляды регистратур на определение неправильного использования DNS, ограниченные возможности регистратур в принятии мер в отношении угроз безопасности и их опасения в отношении платформы отчетности о случаях злоупотребления доменами, разработанной ICANN.

В ответ GAC опубликовал Заявление о неправильном использовании DNS (18 сентября 2019 года); к нему присоединилась Группа интересов коммерческих пользователей (28 октября 2019 года). В своем Заявлении GAC признает формулировку неправильного использования DNS, составленную группой по анализу CCT: «*намеренное введение в заблуждение, потворствование или нежелательные действия, для которых активно используются DNS и (или) процедуры регистрации доменных имен*» и которые в техническом плане могут принимать форму угроз безопасности, таких как «*вредоносное ПО, фишинг и ботнеты, а также спам при его использовании в качестве способа совершения этих видов злоупотреблений*». GAC признает, что Соглашение об администрировании нового gTLD отражает это понимание в спецификации 11, в частности, в разделах 3a[15] и 3b[16].

После опубликования Заявления GAC о неправильном использовании DNS (18 сентября 2019 года) несколько **ведущих регистратур и регистраторов gTLD предложили для добровольной реализации** Концепцию борьбы со злоупотреблениями (17 октября 2019 года). Примечательно, что данная Концепция включает в сферу возможных действий со стороны ее сторонников определенные формы «злоупотребления контентом веб-сайта», которые она считает

---

[15] В разделе 3a спецификации 11 предусмотрено следующее: *«Оператор регистратуры включает в Соглашение между регистратурой и регистратором требование, обязывающее регистраторов включать в свои регистрационные соглашения положение, запрещающее владельцам зарегистрированных имен распространять вредоносное ПО, использовать в злонамеренных целях ботнеты, заниматься фишингом, пиратством, нарушать авторские права и права на товарные знаки, вести мошенническую или вводящую в заблуждение деятельность, распространять контрафактную продукцию и вести прочую деятельность, идущую вразрез с соответствующим законодательством. Кроме того, в этом положении должны быть указаны меры пресечения такой деятельности (соответствующие законодательству и любым сопряженным процедурам), в том числе приостановка работы доменного имени».*

[16] В разделе 3b спецификации 11 предусмотрено следующее: *«Оператор регистратуры обязан периодически проводить технический анализ того, не используются ли домены в TLD для создания угроз безопасности, таких как фарминг, фишинг, вредоносное ПО и ботнеты. Оператор регистратуры составляет статистические отчеты о количестве обнаруженных угроз безопасности и мерах, принятых в результате периодических проверок безопасности. Оператор регистратуры хранит такие отчеты в течение всего срока действия Соглашения, кроме случаев, когда более короткий срок предусмотрен законом или одобрен ICANN, и предоставляет их корпорации ICANN по запросу».*

«настолько вопиющими, что сторона по контракту должна действовать, когда ей предоставляется конкретное и достоверное уведомление». Со времени ее опубликования и обсуждения на ICANN66 список подписавших эту концепцию расширился и теперь включает в себя других ведущих регистраторов и поставщиков услуг регистратуры, а также ряд мелких игроков отрасли.

18 июня 2020 года председатели **групп заинтересованных сторон регистратур и регистраторов** (известной под общим названием «Палата сторон, связанных договорными обязательствами GNSO» или CPH) сообщили лидерам сообщества о **принятии** определения неправильного использования DNS, которое точно отражает Концепцию борьбы со злоупотреблениями:

> *Неправильное использование DNS состоит из пяти широких категорий вредоносной активности, той мере, в которой они пересекаются с DNS: вредоносное ПО, ботнеты, фишинг, фарминг и спам, когда он служит механизмом доставки для других форм неправильного использования DNS* [ссылка на определения каждого из этих видов деятельности в документе Операционные подходы, нормы, критерии, механизмы Организации по вопросам интернет-политики и юрисдикции].

Это определение, **похоже, подтверждает то, что группа по анализу CCT назвала существующим консенсусом в отношении того, что представляет собой «нарушение безопасности DNS»** или «злоупотребление безопасностью инфраструктуры DNS» (Итоговый отчет CCT, стр. 8.) и **соответствует иллюстративному определению GAC «Угрозы безопасности»** в рекомендациях GAC по мерам защиты «Проверки безопасности», применимых ко всем новым gTLD, в Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Пекине (11 апреля 2013 г.), включенных в Соглашение об администрировании домена верхнего уровня (gTLD) в соответствии со Спецификацией 11 3.b.

Центр внимания: Меры безопасности для борьбы с неправильным использованием 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 **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 ICANN по контролю исполнения договорных обязательств**, 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».[17] Вскоре после этого, в ноябре 2018 года, была начата проверка злоупотреблений на уровне инфраструктуры DNS почти **всех регистратур gTLD**, целью которой являлось *«обеспечение соблюдения сторонами, связанными договорными обязательствами, своих обязательств согласно договорам в том, что касается злоупотреблений и угроз безопасности на уровне инфраструктуры DNS»*. В своем отчете о результатах этой проверки (17 сентября 2019 года) ICANN пришла к следующему выводу:

- подавляющее большинство операторов регистратур стремятся противостоять угрозам безопасности DNS.
- Распространенность угроз безопасности DNS сосредоточена в относительно небольшом круге операторов регистратур.
- Некоторые операторы регистратур интерпретируют договорную формулировку спецификации 11 3 (b) таким образом, что это затрудняет формирование суждения о том, являются ли их усилия по снижению угроз безопасности DNS соответствующими и эффективными.

В январе 2021 года отдел ICANN по контролю исполнения договорных обязательств начал проверку **соблюдения регистраторами своих обязательств, связанных с угрозами безопасности DNS.** После разработки совместно с группой заинтересованных сторон-регистраторов запроса информации (в том числе документации по возможным подходам регистраторов к работе с доменами, потенциально использующимися для злоупотреблений), отдел по контролю исполнения договорных обязательств ICANN проводит проверку 127 регистраторов, у которых в отчетах об угрозах безопасности, предоставленных регистратурами во время предыдущего аудита, или в отчете офиса CTO ICANN о злоупотреблениях за ноябрь 2020 года было обнаружено не менее 5 доменных имен. Во время сделанного накануне ICANN70 доклада о работе отдела по контролю исполнения договорных обязательств корпорация ICANN указала, что планирует представить отчет об этой проверке в начале июня 2021 года.

Центр внимания: 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*

[17] 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

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 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 «*национальные правоохранительные органы или органы защиты общественной безопасности в соответствующей юрисдикции*».

В соответствии с рекомендацией 19 группа по анализу CCT отложила выполнение задачи по оценке эффективности данной концепции до следующей проверки[18], поскольку малый срок существования концепции не позволяет оценить ее эффективность.

[18] 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*

Центр внимания: Рассмотрение рекомендаций по результатам проверки CCT, касающихся неправильного использования DNS

Основываясь на своем анализе сложившейся ситуации в том, что касается неправильного использования DNS,[19] в т. ч. учитывая отчет ICANN о механизмах защиты программы New gTLD (15 марта 2016 года) и независимый статистический анализ неправильного использования DNS (9 августа 2017 года), группа проверки конкуренции, потребительского доверия и потребительского выбора рекомендовала в отношении неправильного использования 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)

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».[20]

В свете рекомендации Правлению ICANN в Коммюнике по результатам заседаний GAC в Монреале (6 ноября 2019 года) *не приступать к новому раунду gTLD до полного выполнения рекомендаций [...], которые были определены в качестве «предварительных условий» или имеют «высокий приоритет»*, и ответа Правления на эту рекомендацию (26 января 2020 года) PSWG продолжает следить за рассмотрением важнейших рекомендаций группы по анализу CCT (6 сентября 2018 года), направленных на: внедрение договорных положений, стимулирующих заблаговременное принятие мер по борьбе со злоупотреблениями (рек. 14) и предотвращение систематического использования регистраторов или регистратур для злоупотребления DNS (рек. 15); улучшение исследования злоупотребления DNS (рек. 16); повышение достоверности данных WHOIS (рек. 18) и эффективное рассмотрение жалоб на несоблюдение договорных обязательств (рек. 20).

PSWG GAC также рассмотрела резолюцию Правления продолжить выполнение подготовленного ICANN плана выполнения (23 августа 2019 года) рекомендаций CCT, которые были приняты в

---

[19] См. раздел 9 «Меры безопасности» (стр. 88) в итоговом отчете по результатам проверки CCT (8 сентября 2018 года)

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

оценочном отчете о действиях Правления ICANN (1 марта 2019 года). GAC прокомментировал (21 октября 2019 года) этот план и отметил некоторые недостатки в отношении важных рекомендаций по борьбе с неправильным использованием DNS, включая опубликование данных о цепочке сторон, ответственных за регистрацию доменных имен в gTLD (рек. 17), более подробную информацию о жалобах на несоблюдение договорных обязательств (рек. 21), меры безопасности, соразмерные предлагаемым услугам, которые включают сбор конфиденциальной медицинской и финансовой информации (рек. 22).

После принятия сторонами, связанными договорными обязательствами, определения неправильного использования DNS, **GAC запросил разъяснения у Правления ICANN во время ICANN68** (см. материалы заседания GAC и Правления от 24 июня 2020 года) в связи с выполнением рекомендации 14 CCT-RT (*ICANN должна провести переговоры о положениях договора, предусматривающих финансовые стимулы для принятия договаривающимися сторонами активных мер по борьбе с неправильным использованием*) относительно статуса и плана по содействию усилиям сообщества по разработке определения «неправильного использования» и информированию Правления о дальнейших действиях по этой рекомендации. GAC записал в протоколе ICANN68, что «*Правление продолжит поддерживать диалог с сообществом, как это делало раньше, путем содействия региональных и сквозных дискуссий сообщества, проведения исследований и разработки инструментов, помогающих информировать обсуждения в сообществе, и путем предоставления докладчиков по запросу*».

Во время конференции ICANN68 рабочая группа PSWG отметила вместе с заинтересованными сторонами ALAC, что прогресс в реализации принятой рекомендации CCT-RT и в рассмотрении ожидающей рекомендации остается неясным. Неудовлетворенность была также выражена в сообщении (29 апреля 2020 года) **Рабочей группы GNSO по процессу разработки политики в отношении последующих процедур, применимых к новым gTLD**, о том, что она «*не планирует давать какие-либо рекомендации, касающиеся борьбы со злонамеренным использованием доменных имен, за исключением заявления о том, что любые такие будущие усилия должны охватывать как существующие, так и новые gTLD (а, возможно, и ccTLD)».* Это несмотря на соответствующие рекомендации, адресованные ей группой по анализу CCT и поддержанные действиями Правления ICANN по этим рекомендациям, а также коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Монреале, в котором приведена рекомендация (6 ноября 2019 года), и дальнейший вклад GAC, как указано в Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) на ICANN67 (16 марта 2020 года).

В своем итоговом отчете (1 февраля 2021 года) Рабочая группа GNSO по процессу разработки политики в отношении последующих процедур, применимых к новым gTLD, подтвердила свое решение[21]. В связи с этим GAC выразил серьезную озабоченность в Комментариях GAC (29 сентября 2020 года) к проекту итогового отчета указанной РГ по PDP и отметил, что ожидает принятия Советом GNSO незамедлительных мер по данному вопросу.

[21] См. итоговый отчет рабочей группы по PDP Sub Pro, Рекомендация № 9.15 (стр. 42)

Центр внимания: Обсуждение разработки политики GNSO по предотвращению неправильного использования DNS

В соответствии с предварительным решением РГ по PDP в отношении последующих процедур, применимых к новым gTLD, не давать никаких рекомендаций касательно положений о неправильном использовании DNS в будущих соглашениях об администрировании новых gTLD, **Совет GNSO обсудил** в ходе совещания 21 марта 2020 года **возможность создания Сквозной рабочей группы сообщества (CCWG)** по вопросам неправильного использования DNS и, возможно, последующего PDP GNSO, если потребуются новые контрактные требования.

Не обсуждалось неофициальное предложение руководства GAC (12 мая 2020 года) рассмотреть возможность обсуждения типа «рыбак рыбака» среди соответствующих экспертов, включая операторов ccTLD, для охвата любых дальнейших усилий по разработке политики.

По состоянию на 20 мая 2021 года этот вопрос все еще имеет статус «Не запланировано» в реестре задач и решений Совета GNSO, и Совету GNSO «*необходимо определить следующие шаги касательно неправильного использования DNS, если таковые требуются*».

В период после ICANN70 и телеконференции руководства GAC и GNSO, проведенной перед ICANN70 (8 марта 2021 года), а также состоявшейся на ICANN70 встречи GAC с GNSO (24 марта 2021 года), Совет GNSO обсуждал во время своих последних ежемесячных совещаний полученные материалы по вопросу неправильного использования DNS:

- 22 апреля 2021 года созданная Палатой сторон, связанных договорными обязательствами, GNSO **группа по борьбе с неправильным использованием DNS** рассмотрела различные инициативы, предпринятые этими сторонами за последние несколько лет, о которых GAC ранее получил информацию от PSWG. Что касается текущей и будущей работы, были упомянуты несколько инициатив:
    - Сотрудничество с PSWG GAC для масштабного решения проблемы вредоносного ПО и ботнетов
    - Рассмотрение регистраторами мотивационных программ
    - Информационно-разъяснительная работа с другими группами интересов ICANN, включая встречу в формате «вопрос-ответ», опрос сообщества и другие информационные ресурсы
- 20 мая 2021 года Совет GNSO заслушалинформационные доклады лидеров SSAC о недавно опубликованном отчете SAC115, в котором предлагается основанный на функциональной совместимости подход к решению проблемы со злоупотреблениями в DNS (19 марта 2021 года). Во время этой встречи не состоялось последующее обсуждение Советом GNSO документа SAC115 или дальнейших более широких шагов по борьбе с неправильным использованием DNS.

Центр внимания: Отчеты 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 с неправильным использованием DNS в период между конференциями ICANN57 (ноябрь 2016 года) и ICANN60 (ноябрь 2017 года).[22]

Цель проекта DAAR — «*информирование сообщества ICANN о деятельности, связанной с угрозами безопасности; эти данные сообщество ICANN может затем использовать для принятия обоснованных 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.[23]

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 письме группы M3AAWG[24] 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.

Недавно регистратуры в открытом письме (19 августа 2019 г.) в офис технического директора ICANN упомянули о необходимости «*проанализировать DAAR с целью рекомендовать OCTO усовершенствования, чтобы гарантировать, что DAAR лучше выполняет свое предназначение и служит сообществу ICANN ценным ресурсом*». Регистратуры признают, что «*некоторые члены сообщества могут использовать данные, представленные на платформе отчетности ICANN о случаях злоупотребления доменами (DAAR), для поддержки заявлений о системном или широко распространенном неправильном использовании DNS*», но вместе с тем они верят, что «*инструмент имеет значительные ограничения, на него нельзя полагаться для точного и надежного представления свидетельств угроз безопасности, и он еще не достигает своих целей*».

Группа заинтересованных сторон-регистратур доложила о своей работе в Отчете рабочей группы по вопросам DAAR (9 сентября 2020 года), в ответ на который технический директор ICANN сообщил (30 сентября 2020 года): «*большинство рекомендаций в письме*

---

22 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.

23 Подробнее см. здесь: https://www.icann.org/octo-ssr/daar-faqs

24 Рабочая группа по борьбе со злоупотреблением рассылкой сообщений

подчеркивают важность улучшения информационного взаимодействия в том, что касается данных, экспортируемых из системы DAAR, поскольку Рабочая группа считает это взаимодействие в принципе неясным с точки зрения как текущей методологической документации DAAR, так и текста ежемесячных отчетов DAAR. В то время как большинство рекомендаций сфокусированы на конкретных изменениях в отчете, некоторые (например, рекомендация 3, которая требует измерять «интенсивность» сообщений о неправильном использовании) могут потребовать более длительного исследования и анализа».

Во время представления актуальной информации OCTO для GAC (24 февраля 2021 года) технический директор ICANN обсудил планы на будущее по развитию DAAR: добавление большего количества ccTLD в сферу действия DAAR, продолжение сотрудничества с рабочей группой RySG DAAR для изучения решений для преодоления проблем доступа к данным WHOIS и определения показателей на уровне регистратора, в числе которых: ежедневные запросы к WHOIS только для заблокированных доменов, случайная выборка доменов или получение разрешения на использование данных путем массового доступа к регистрационным данным (BRDA).

Текущее положение дел

Далее в обратном хронологическом порядке представлены позиции GAC по следующим вопросам:

- Комментарии GAC (8 апреля 2021 года) по поводу итогового отчета группы по анализу SSR2, представленные на рассмотрение Правления ICANN
- В коммюнике по результатам заседаний GAC на конференции ICANN70 (25 марта 2021 года) отмечается, что «*Проблемы неправильного использования DNS необходимо решить в сотрудничестве с сообществом ICANN и корпорацией ICANN до начала второго раунда создания новых gTLD. GAC поддерживает подготовку положений договоров, применимых ко всем gTLD, для повышения эффективности реагирования на неправильное использование DNS. GAC также подчеркивает важность принятия мер, которые позволили бы обеспечить соблюдение положений договоров в ICANN регистратурами, регистраторами и поставщиками услуг сохранения конфиденциальности и регистрации через доверенных лиц, в том числе аудиторских проверок. GAC приветствует недавно запущенный проект «Институт по борьбе с неправильным использованием DNS» и призывает сообщество объединить усилия для принятия комплексных мер, направленных на решение проблемы неправильного использования DNS*».
- В коммюнике по результатам заседаний GAC на конференции ICANN69 (23 октября 2020 года) отмечалась убежденность GAC в том, что «*сейчас есть твердая и широкая поддержка конкретных шагов, которые необходимо предпринять для формирования основных компонентов эффективной борьбы с неправильным использованием DNS*» в свете растущей динамики и конструктивного диалога в сообществе ICANN (см. раздел IV.2, стр. 6).

- В коммюнике по результатам заседаний GAC на конференции ICANN68 (27 июня 2020 года) отмечалось, «*что новые усилия по борьбе с неправильным использованием DNS не должны заменять, а скорее должны дополнять существующие инициативы по повышению достоверности регистрационных данных, такие как Система учета достоверности данных, и внедрять политику в отношении услуг сохранения конфиденциальности и регистрации через доверенных лиц, реализация которой в настоящее время приостановлена*» (см. раздел IV.3, стр. 7)
- Комментарий GAC (3 апреля 2020 года) по поводу проекта отчета группы по анализу SSR2
- Комментарий GAC относительно итоговых рекомендаций по результатам работы RDS-WHOIS2 (23 декабря 2019 года)
- Заявление GAC о неправильном использовании DNS (18 сентября 2019 года)
- Комментарии GAC относительно итогового отчета об анализе CCT (11 декабря 2018 года)
- Комментарий GAC (16 января 2018 года) к новым разделам в проекте отчета группы по анализу конкуренции, потребительского доверия и потребительского выбора (27 ноября 2017 года)
- Комментарий GAC к отчету «Статистический анализ злоупотреблений DNS в gTLD» (19 сентября 2017 года)
- Комментарий GAC относительно отчета «Механизмы защиты от неправильного использования DNS, предусмотренные в рамках Программы New gTLD» (21 мая 2016 года)
- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) 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)
- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Копенгагене (15 марта 2017 года), в т. ч. рекомендация по борьбе со злоупотреблениями с запросом ответов на вопросы оценочного отчета GAC в дополнение к приложению 1 к коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Хайдарабаде (стр. 11–32)
- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Хайдарабаде (8 ноября 2016 года), в т. ч. рекомендация по борьбе со злоупотреблениями с запросом ответов на вопросы приложения 1 — Вопросы к Правлению ICANN о борьбе ICANN и сторон, связанных договорными обязательствами, с неправильным использованием DNS (стр. 14–17)
- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Пекине (11 апреля 2013 года), в частности меры, направленные на проверку безопасности, распространяющиеся на все новые gTLD (стр. 7)
- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Дакаре (27 октября 2011 года), раздел III. Рекомендации правоохранительных органов

- Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Найроби (10 марта 2010 года), раздел VI. Рекомендации правоохранительных органов в отношении комплексной проверки
- Рекомендации правоохранительных органов в отношении поправок к соглашению с регистраторами (1 марта 2012 года)
- Рекомендации правоохранительных органов в отношении комплексной проверки (октябрь 2009 года)

Вопросы для рассмотрения представителями GAC

При подготовке к этому и другим заседаниям GAC на ICANN71 и будущих конференциях было принято во внимание, что представителям GAC принесло бы пользу более глубокое обсуждение различных тем ICANN в своем собственном правительстве или организации. Ниже в качестве проводимого на ICANN71 эксперимента представлено несколько сформулированных в результате коллективной работы персонала корпорации ICANN типовых вопросов, которые представителям GAC следует обсудить при подготовке к заседаниям и обмену информацией на конференции, чтобы способствовать дискуссиям, обмену передовым опытом и, возможно, определению различных подходов или стратегий тех или иных правительств в отношении этих вопросов. Читатели могут использовать приведенные ниже вопросы для придания целенаправленного характера подготовительной работе или для расширения диалога на будущей встрече. Сообщите персоналу поддержки GAC, считаете ли вы такие вопросы полезными при подготовке к конференции.

Что касается контроля за соблюдением положений о противодействии злоупотреблениям, содержащихся в соглашениях с регистратурами и соглашениях об аккредитации регистраторов:

- Есть ли у вашего правительства определение понятия «неправильное использование DNS»? Если да, какова государственная формулировка этого понятия?
- Сталкивались ли государственные органы в вашей стране с доменными именами, которые предположительно используются для совершения злоупотреблений в DNS, и сообщали ли о них соответствующей регистратуре или регистратору? Если да, какая доля отправленных регистратуре или регистратору сообщений о таких доменных именах gTLD была переадресована отделу ICANN по контролю исполнения договорных обязательств в случае неспособности сторон, связанных договорными обязательствами, должным образом своевременно рассмотреть отправленное сообщение в пределах своих возможностей?
- Какая доля имен, предположительно используемых для совершения злоупотреблений в DNS, регистрируется в gTLD по сравнению с ccTLD?
- Ознакомились ли государственные органы вашей страны с опубликованными группой заинтересованных сторон-регистраторов руководящими принципами, где содержится информация, которая может быть полезна при подаче регистраторам жалоб на злоупотребления?

- Знакомы ли государственные органы вашей страны с положениями Соглашения об администрировании домена верхнего уровня (RA) и Соглашения об аккредитации регистраторов (RAA), соблюдение которых контролируется и обеспечивается ICANN? (В частности с разделами 3a и 3b спецификации 11 RA и разделом 3.18 RAA.)
- Какие органы и механизмы правоприменения, по мнению государственных органов вашей страны, имеются у ICANN для противодействия злоумышленному использованию доменов?

Что касается усилий корпорации ICANN по обнаружению угроз безопасности и информированию о них:

- Используемая ICANN платформа отчетности о случаях злоупотребления доменами (DAAR) предназначена для постоянного предоставления сообществу ICANN фактологических, надежных и объективных данных с помощью открытой и проверенной сообществом методологии, которая может применяться с целью создания информационной основы для обсуждения политики. Какие улучшения, по мнению вашего правительства или соответствующих государственных органов, следует внести в DAAR?
- Какие улучшения, по мнению вашего правительства или соответствующих государственных органов, следует внести в созданный ICANN инструмент сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR) для обнаружения вредоносного ПО и фишинга, имеющих отношение к COVID-19?
- Известно ли вашему правительству о результатах этой работы на сегодняшний день, в частности о том, что доказательства проблем, о которых необходимо сообщить связанным договорными обязательствами сторонам, были обнаружены в паре сотен случаев?

Что касается усилий ICANN по поддержке снижения угроз безопасности DNS:

- Считает ли ваше правительство, что ICANN целесообразно сосредоточить внимание на поддержке снижения угроз безопасности DNS в gTLD, как они определены GAC (фишинг, вредоносное ПО, командные и управляющие серверы ботнетов и фарминг, а также спам при его использовании в качестве средства создания других видов угроз безопасности) с учетом содержащегося в Уставе ICANN запрета на регулирование контента и отсутствия юрисдикции в отношении ccTLD?
- Готово ли ваше правительство внести свой вклад в текущие дискуссии сообщества ICANN, которые направлены на определение проблемы и поиск наилучшего способа борьбы с неправильным использованием DNS, будь то добровольное внедрение передовой практики, реализация согласованной политики или сочетание обоих вариантов?
- Какие объективные фактологические данные, по мнению вашего правительства, корпорация ICANN может предоставить для содействия этим дискуссиям в сообществе?

Важнейшие справочные документы

- Документация GAC о неправильном использовании DNS
    - Заседание GAC на ICANN70, посвященное вопросам неправильного использование DNS (23 марта 2020 года)
    - Информационные материалы GAC для конференции ICANN68 о неправильном использовании DNS (18 июня 2020 года)
    - Вопросы GAC о борьбе со злоупотреблениями и проект ответов ICANN (30 мая 2017 года) по рекомендациям из Коммюнике по результатам заседаний GAC в Хайдарабаде (8 ноября 2016 года) и продолжение по этому вопросу в Коммюнике по результатам заседаний GAC в Копенгагене (15 марта 2017 года)
- Определение неправильного использования DNS (включая мнение заинтересованных сторон отрасли)
    - Определение «неправильного использования DNS», сформулированное сторонами, связанными договорными обязательствами (октябрь 2020 года)
    - Концепция борьбы с неправильным использованием DNS (17 октября 2019 года)
    - Заявление GAC о неправильном использовании DNS (18 сентября 2019 года)
- Итоговый отчет о результатах проверки SSR2 (25 января 2021 года)
- Проверка RDS-WHOIS2
    - Оценочный отчет о решениях Правления ICANN в отношении окончательных рекомендаций по итогам проверки RDS-WHOIS2 (25 февраля 2020 года)
    - Окончательные рекомендации по итогам проверки RDS-WHOIS2 (3 сентября 2019 года)
- Анализ конкуренции, потребительского доверия и потребительского выбора
    - Оценочный отчет о действиях Правления ICANN (22 октября 2020 года) по 11 отложенным рекомендациям CCT из 17 и соответствующие результаты подробной оценки , предоставленные корпорацией ICANN
    - Оценочный отчет о решениях Правления ICANN в отношении итоговых рекомендаций по результатами проверки CCT (1 марта 2019 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)
    - Статистический анализ злоупотреблений DNS в gTLD (9 августа 2017 года)

Управление документом

Совещание	Виртуальный форум по формированию политики ICANN71, 14–17 июня 2021 года
Название	Информационные материалы GAC к конференции ICANN71 — Заседание № 3 — Борьба с неправильным использованием DNS
Распространение	Члены GAC (до заседания) и общественность (после заседания)
Дата распространения	Версия 1: 1 июня 2021 года