ICANN | GAC
Governmental Advisory Committee

ICANN 68
VIRTUAL POLICY FORUM
22–25 June 2020

Борьба с неправильным использованием DNS

Заседания 2, 8

Содержание

Цели заседания

GAC обсудит последние события, связанные с неправильным использованием DNS, в частности в контексте кризиса COVID-19, в связи с общим пленарным заседанием сообщества, которое запланировано на эту тему во время ICANN68. Эта сессия также даст возможность рассмотреть и обсудить важные события в области предотвращения и смягчения последствий неправильного использования DNS и угроз безопасности.

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 преступная 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 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 неправильного использования DNS 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).

- **В рамках программы New gTLD,** [2]принятие корпорацией ICANN своего меморандума 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 г.) в рамках подготовки к предусмотренной Уставом проверке конкуренции, потребительского выбора и потребительского доверия (CCT), рекомендации которой были представлены 8 сентября 2018 года.

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

[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 DNS-сервера, 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

- До создания рабочей группы GAC по обеспечению общественной безопасности (PSWG) **представители правоохранительных агентств** 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 GAC**.
- **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 **офис технического директора** ICANN разработал платформу отчетности о случаях злоупотребления доменами (DAAR) и формирует 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.

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 существующие отраслевые практические методики по борьбе с неправильным использованием 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].

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

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

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 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 количества регистраций в соответствующих доменах, включая небольшой процент[6] в поддержку различных конъюнктурных мошеннических целей.

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[7].

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 и сообщение о неправильном использовании DNS (с точки зрения осведомленности и транспарентности):**
  Как обеспечить обнаружение неправильного использования DNS и донесение информации об этом до соответствующих заинтересованных сторон, в т. ч. потребителей и интернет-пользователей?
- **Предотвращение и смягчение последствий неправильного использования 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 интернет-пользователей может решить принять активное участие в продвижении дискуссии по этим вопросам (подробно освещенным в данном брифинге) ради достижения прогресса в повышении эффективности предотвращения и устранения злоупотреблений.

---

[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 злоупотреблением рассылкой сообщений (18 октября 2018 года)

[6] Как сообщается лидерами групп заинтересованных сторон-регистраторов в докладе GAC 9 апреля 2020 года

[7] 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 на ICANN68

1. **Провести обзор уроков,** уже извлеченных **из неправильного использования DNS, связанного с COVID-19,** по сообщениям заинтересованных сторон, включая государственные органы, регистраторов, операторов ccTLD и корпорацию ICANN, **и подготовиться к участию сообщества ICANN в случае необходимости,** начиная с общего пленарного заседания по вопросам неправильного использования DNS и злонамеренных регистраций во время COVID-19, запланированного на 22 июня 2020 года в рамках ICANN68.

2. **Обдумать возможные последующие шаги для решения общих вопросов общественной политики, связанных с неправильным использованием DNS,** как указано в предыдущих рекомендациях GAC, и, **в частности, рассмотреть дальнейшие совместные действия** с Советом GNSO, ALAC, ccNSO и, возможно, Правлением ICANN **в отношении возможных путей выполнения рекомендаций CCT по неправильному использованию DNS до запуска последующих раундов новых gTLD** в соответствии с коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Монреале и соответствующей рекомендацией (6 ноября 2019 г.).

3. **Обсудить состояние** рассмотрения и реализации **рекомендаций, относящихся к неправильному использованию DNS, выпущенных в рамках проверок CCT и RDS-WHOIS2,** в свете действий Правления ICANN, о которых сообщается в следующих документах:
    a. Оценочный отчет о действиях Правления в отношении рекомендаций по итогам проверки CCT (1 марта 2019 года)
    b. Оценочный отчет о действиях Правления в отношении рекомендаций по итогам проверки RDS-WHOIS2 (25 февраля 2020 года)

4. **Рассмотреть прогресс в основных усилиях по смягчению последствий неправильного использования DNS в сообществе ICANN** и, в частности, сторонами, связанными договорными обязательствами, операторами ccTLD и корпорацией ICANN, в том числе с целью продвижения повышенных стандартов в практике и договорах:
    a. **Реализация добровольных мер регистраторами и регистратурами gTLD** согласно отраслевой концепции борьбы со злоупотреблениями
    b. **Реализация профилактических мер против злоупотреблений операторов ccTLD**, которые могли дать информацию для совершенствования практической деятельности регистратур gTLD
    c. **Аудит соблюдения договорных обязательств регистраторами** относительно угроз безопасности DNS, которые должны были последовать за выводами соответствующего аудита регистратур
    d. Усовершенствование платформы отчетности ICANN о случаях злоупотребления доменами (DAAR), как ранее обсуждалось регистратурами, GAC и SSAC

Важные изменения

Обзор последних событий

- **Кризис, связанный с COVID-19, привел к взаимодействию между GAC и заинтересованными сторонами**, которое вывело на первый план различные **усилия по реагированию и координации ответа** на мошеннические и преступные действия:
    - **Руководство GAC** сообщило на обсуждении (9 апреля) по запросу руководителей Группы заинтересованных сторон-регистраторов (RrSG) и дополнительно обсудило этот вопрос в совместной телеконференции руководства (3 июня 2020 г.) в рамках подготовки к ICANN68.
    - Отвечая, в частности, на потенциальные проблемы с мошенническими действиями под предлогом COVID-19, доклад **регистраторов** упоминает об оценке мошенничества в соответствующей юрисдикции и необходимости обратиться за помощью к государственным органам. RrSG задокументировала общий подход регистраторов к кризису COVID-19, ориентированный на благо ее членов.
    - **Членам GAC было предложено поделиться соответствующими ресурсами**, предоставленными соответствующими государственными органами, такими как правоохранительные агентства (ФБР в США, NCA в Великобритании, Европол) и агентства по защите прав потребителей (FTC в США)
    - **Европейская комиссия** сообщила о текущих усилиях, предпринимаемых в сотрудничестве с государствами-членами ЕС, Европолом, ccTLD и регистраторами, для облегчения подготовки отчетов, их рассмотрения и передачи 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 государств-членов.
    - **Операторы ccTLD** по всему миру должны проинформировать GAC (4-5 июня 2020 г.) об уроках, которые они извлекли из своей деятельности во время кризиса
    - Краткий брифинг для GAC со стороны **офиса технического директора ICANN** (OCTO), который планируется провести до начала ICANN68, как ожидается, проиллюстрирует инициативы и ресурсы ICANN, предназначенные для поддержки ответных действий сторон, связанных договорными обязательствами

- Тем временем, **стороны, связанных договорными обязательствами, Консультативный комитет ICANN по безопасности и стабильности (SSAC) и корпорация ICANN начали новую работу**, связанную с устранением угроз безопасности:

- Как сообщила рабочая группа GAC по обеспечению общественной безопасности во время конференции ICANN67, **группа заинтересованных сторон-регистраторов** опубликовала Руководство по отчетности регистраторов о злоупотреблениях
- Концепцию борьбы с неправильным использованием DNS (17 октября 2019 г.), предложенную в качестве **добровольной инициативы ведущих участников отрасли DNS**, сейчас подписали 56 сторон (по состоянию на 29 марта 2020 года).
- **SSAC** инициировала создание рабочей группы по неправильному использованию DNS, в которую был приглашен представитель PSWG.
- **Корпорация ICANN** в рамках реализации Стратегического плана на 2021-2025 ФГ объявила о создании технической исследовательской группы в рамках Инициативы по содействию безопасности DNS (6 мая 2020 г.) 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.

- После конференции ICANN66 **в сообществе ICANN были рассмотрены новые рекомендации, связанные с неправильным использованием DNS**, при этом некоторые из них получили отклики со стороны GAC, а некоторые могут быть предметом последующих действий GAC:
  - После того, как **группа по анализу RDS-WHOIS2** опубликовала окончательные рекомендации (3 сентября 2019 г.), важность которых для смягчения последствий неправильного использования DNS была подчеркнута в Комментариях GAC (23 декабря 2019 г.), были рассмотрены Правлением ICANN в соответствии с оценочным отчетом о действиях Правления (25 февраля 2020 г.) и в рамках резолюций 2020.02.25.01 - 2020.02.25.06: 15 рекомендаций были приняты, 4 переведены в состояние ожидания, 2 переданы в GNSO и 2 отклонены.
  - **Группа по анализу SSR2** представила Проект отчета (24 января 2020 г.), 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. Окончательные рекомендации SSR2 RT теперь ожидаются к октябрю 2020 года (согласно недавнему обсуждению)
  - **Рабочая группа GNSO по процессу разработки политики в отношении последующих процедур, применимых к новым gTLD** недавно сообщила (29 апреля 2020 г.), что «*не планирует давать какие-либо рекомендации в отношении смягчения последствий злоупотреблений доменными именами, за исключением заявления о том, что любые такие будущие усилия должны*

применяться как к существующим, так и к новым gTLD (и, возможно, к 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 г.), и дальнейший вклад GAC, как указано в Коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) на ICANN67 (16 марта 2020 г.). На недавнем заседании Совета GNSO (21 марта 2020 г.) обсудили возможность создания сквозной рабочей группы сообщества (CCWG) и, возможно, последующего PDP GNSO, если потребуются новые контрактные требования. Не обсуждалось неофициальное предложение руководства GAC (12 мая 2020 г.) рассмотреть возможность обсуждения «рыбак рыбака» среди соответствующих экспертов, включая операторов ccTLD, для охвата любых дальнейших усилий по разработке политики.

Проблемы - определение неправильного использования DNS

Как подчеркивалось в ходе прошедшего недавно 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.[8]

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».*[9]

Недавно **отдел ICANN по контролю исполнения договорных обязательств упомянул «злоупотребления инфраструктурой DNS» и «угрозы безопасности»** 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*»[10], 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, 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).

После резолюции Правления от 1 марта 2019 года, которой корпорации ICANN было поручено «*способствовать усилиям сообщества по выработке определения термина*

---

[8] 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.

[9] 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.)

[10] 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».*

«злоупотребление», чтобы создать основу для дальнейших действий по данной рекомендации»[11], а также усилий отдела защиты прав потребителей корпорации ICANN, **ожидается, что дальнейшее обсуждение определения понятия «злоупотребления» состоится до начала и в ходе конференции ICANN66**, которая пройдет в Монреале.

В частности, 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 г.), 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), к нему присоединилась Группа интересов коммерческих пользователей (28 октября).

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

Проблемы – информированность и транспарентность: взаимодействие с сообществом по проблеме неправильного использования DNS

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**. Совсем недавно лидеры организаций поддержки и консультативных комитетов ICANN (SO/AC) и ALAC приняли участие в этом мероприятии.

- 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 с неправильным использование DNS, в частности, с фишингом, а также такие шаблоны поведения регистраторов и регистратур, как частая смена TLD, 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[12].

- В ходе конференции ICANN66 в Монреале (6 ноября 2019 г.) сообщество ICANN провело совместное пленарное заседание по неправильному использованию DNS
- Во время виртуальной конференции ICANN67 (9 марта 2020 г.) ALAC провел два заседания, в которых удаленно приняли участие многие члены сообщества ICANN; на одном было введение в проблему неправильного использования DNS (включая учебное видео), а на втором был дан практический обзор случаев правоприменения контрактных требований в ответ на типичные случаи неправильного использования DNS

Проблемы – информированность и транспарентность: исследования неправильного использования DNS

Ряд мер по защите от злоупотреблений DNS были встроены в программу ввода новых gTLD посредством новых требований,[13] 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.

[12] 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)

[13] 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

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)
- 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.

17 октября 2019 года консалтинговой компанией (Interisle Consulting Group) было опубликовано исследование Преступное злоупотребление массовой регистрацией доменных имен и доступ к контактной информации, которое имеет непосредственное отношение к текущим дискуссиям в сообществе; в исследовании затронуты следующие вопросы:

- Как киберпреступники используют услуги массовой регистрации, чтобы задействовать большое количество доменных имен для своих атак.
- Влияние временной политики ICANN по редактированию информации о контактах Whois в соответствии с GDPR на расследования киберпреступлений
- Рекомендации по политике для корпорации ICANN и соображения сообщества

Проблемы – 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 с неправильным использованием DNS в период между конференциями ICANN57 (ноябрь 2016 года) и ICANN60 (ноябрь 2017 года).[14]

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.[15]

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[16] 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*».

Проблемы - эффективность: текущие 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:

---

[14] 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.

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

[16] Рабочая группа по борьбе со злоупотреблением рассылкой сообщений

- 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 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»*.[17] Вскоре после этого, в ноябре 2018 года, была начата проверка злоупотреблений на уровне инфраструктуры DNS почти всех gTLD, целью которой было *«обеспечение соблюдения*

[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

сторонами, связанными договорными обязательствами, своих обязательств согласно договорам в том, что касается злоупотреблений и угроз безопасности на уровне инфраструктуры DNS». В своем отчете о последней проверке (17 сентября 2019 г.) 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.

Стороны, связанные договорными обязательствами, возражали против таких проверок, считая, что они выходят за рамки их договорных обязательств.[18] Корпорация ICANN указала, что она начнет аудит регистраторов, ориентированный на угрозы безопасности DNS.

[18] 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 с неправильным использованием 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*»

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 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 проверки конкуренции, потребительского доверия и потребительского выбора отложила выполнения задачи по проведению оценки эффективности данной концепции до последующей проверки[19], поскольку концепция существует слишком недолго, чтобы оценить ее эффективность.

Эффективность. профилактические меры и недопущение систематических злоупотреблений

Основываясь на своем анализе сложившейся ситуации в том, что касается неправильного использования DNS,[20] 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:

---

[19] 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*

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

- 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».[21]

Текущее положение дел

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

- Комментарий GAC (3 апреля 2020 года) по поводу проекта отчета группы по анализу SSR2
- Комментарий GAC (23 декабря 2019 года) относительно итоговых рекомендаций по результатам работы RDS-WHOIS2
- Заявление GAC о неправильном использовании DNS (18 сентября 2019 года)
- Комментарий GAC (11 декабря 2018 года) относительно итоговых рекомендаций по результатам проверки CCT
- 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 к первоначальному отчету «Статистический анализ злоупотреблений DNS в 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

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

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)

Важнейшие справочные документы

- Оценочный отчет о решениях Правления ICANN в отношении окончательных рекомендаций по итогам проверки RDS-WHOIS2 (25 февраля 2020 года)
- Оценочный отчет о решениях Правления ICANN в отношении итоговых рекомендаций по результатами проверки конкуренции, потребительского доверия и потребительского выбора (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)
- Вопросы GAC о борьбе со злоупотреблениями и проект ответов ICANN (30 мая 2017 года) по рекомендациям из коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Хайдарабаде (8 ноября 2016 года) и продолжение по этому вопросу в коммюнике по результатам заседаний Правительственного консультативного комитета (GAC) в Копенгагене (15 марта 2017 года)

Управление документом

Совещание	Виртуальный форум по формированию политики ICANN68, 22–25 июня 2020 года
Название	Борьба с неправильным использованием DNS
Рассылка	Члены GAC (до заседания) и общественность (после заседания)
Дата распространения	Версия 1: 3 июня 2020 года