
Борьба со злоупотреблениями DNS

Заседание 7

Содержание

Задача заседания	стр. 1	Предложение руководства по 1 действиям GAC	Текущее положение дел и последние события	стр. 2	Важнейшие справочные документы	стр. 7
------------------	--------	--	---	--------	--------------------------------	--------

Задачи заседания

Задача этого заседания — продолжить рассмотрение в GAC инициатив корпорации ICANN и сообщества ICANN по предотвращению и сокращению масштабов злоупотреблений DNS. GAC будет проинформирован о последних событиях, в том числе о новом инструменте информирования о злоупотреблениях (NetBeacon), разработанном по рекомендациям SSAC, и, возможно, о результате рассмотрения подгруппой GNSO мер в области политики, которые следует принять в данном вопросе. Также на данном заседании можно будет возобновить обсуждение возможного взаимодействия GAC с группами заинтересованных сторон для улучшения договорных положений ICANN и обеспечения их соблюдения применительно к злоупотреблению DNS.

Предложение руководства по действиям GAC

- 1. Проанализировать ход выполнения мероприятий корпорации ICANN** в отношении злоупотреблений DNS в рамках программ «Борьба с угрозами безопасности системе доменных имен (DNS)» и «Соблюдение договорных обязательств», о чем в последний раз сообщалось на брифинге корпорации ICANN для GAC перед проведением конференции ICANN74.¹
- 2. Оценить успехи обсуждений в сообществе ICANN и работу по выполнению рекомендаций относительно злоупотреблений DNS**, включая обсуждения небольшой группы GNSO по теме злоупотреблений DNS² и NetBeacon (ранее централизованный

¹ См. <https://gac.icann.org/sessions/icann-org-preicann74-oral-briefing-for-the-gac> (31 мая 2022 года) [требуется авторизация]

² Там же

инструмент информирования о злоупотреблениях) Института по борьбе со злоупотреблениями DNS³.

Текущее положение дел и последние события

Обсуждения в сообществе и конкретные шаги, предпринятые на сегодняшний день

- На последних конференциях ICANN руководители Рабочей группы GAC по обеспечению общественной проводили брифинги для GAC по вопросу злоупотреблений DNS⁴ в соответствии с [планом работы PSWG на 2020–2021 годы](#) и ее стратегической целью № 1: нарастить потенциал в сфере борьбы со злоупотреблениями DNS и киберпреступностью.
 - GAC рассмотрел доступные регистраторам и регистраторам меры по предотвращению злоупотреблений DNS, в частности роль политики регистрации (включая верификацию пользователей) и стратегий ценообразования как ключевых факторов, определяющих количество злоупотреблений в конкретном TLD.
 - GAC также изучил текущие или возможные инициативы по более эффективному противодействию злоупотреблениям DNS на уровне Правления ICANN и корпорации ICANN⁵, в том числе пересмотр договоров ICANN с регистраторами и регистраторами, обеспечение соблюдения существующих требований, выполнение соответствующих рекомендаций по итогам проверок CCT и SSR2, а также рекомендаций по политике в отношении провайдеров услуг сохранения конфиденциальности и регистрации через доверенных лиц, повышение достоверности регистрационных данных и публикация более подробных сведений о злоупотреблениях доменами.
 - В [Коммюнике по результатам заседаний Правительственного консультативного комитета \(GAC\) на конференции ICANN72](#) (1 ноября 2021 года) GAC подчеркнул **«необходимость совершенствования требований к контрактам для более эффективного решения проблемы злоупотребления DNS. В связи с этим, роль ICANN согласно Уставу включает в себя надлежащий учет проблем правительств и государственных органов в сфере общественной политики и действия на благо общества. Устав также уполномочивает ICANN во исполнение своей миссии вести переговоры по заключению соглашений, включая обязательства по обязательствам по обеспечению общественных интересов. Таким образом, ICANN имеет все возможности для проведения переговоров по улучшению существующих контрактов с целью более эффективного противодействия злоупотреблениям DNS, как об этом сообщили GAC и другие заинтересованные стороны, выступающие в защиту общественных интересов»**.

³ См. https://dnsabuseinstitute.org/centralized_abuse_reporting_update/ (5 апреля 2022 года)

⁴ См. материалы соответствующих пленарных заседаний GAC на [ICANN66](#), [ICANN68](#), [ICANN69](#), [ICANN70](#), [ICANN71](#) и ICANN72

⁵ См. [протоколы ICANN66](#), [Коммюнике по результатам заседаний GAC на ICANN68](#) и [протоколы, Коммюнике по результатам заседаний GAC на ICANN69](#) и [протоколы, Коммюнике по результатам заседаний GAC на ICANN70](#) и [протоколы, Коммюнике по результатам заседаний GAC на ICANN71](#) и [протоколы](#).

- В ходе ICANN73 GAC рассмотрел исследование злоупотреблений DNS, опубликованное Еврокомиссией (см. [Отчет](#) и [Техническое приложение](#) к нему, 31 января 2022 года), и отметил в [Коммюнике GAC по результатам ICANN73](#): «В этом исследовании приведено множество ценных ситуационных исследований, разъясняются различные компоненты экосистемы интернета и приведены рекомендации в отношении действий различных сторон (напр., регистратур, регистраторов, реселлеров, поставщиков услуг хостинга, владельцев доменов и т.д.) в связи со злоупотреблениями DNS на различных уровнях системы доменных имен»
- **Небольшая группа Совета GNSO по вопросам злоупотреблений DNS [должна](#)** представить отчет о результатах своей работы после ICANN74 с указанием того, «какие политические усилия, если таковые имеются, Совету GNSO следует предпринять для поддержки усилий, уже предпринимаемых в различных частях сообщества для борьбы со злоупотреблением DNS»
 - 31 января 2022 года Совет GNSO [объявил](#) о создании **небольшой группы GNSO** с целью «обратиться к другим членам сообщества, которые активно высказываются по этой теме (например, Правительственному консультативному комитету [...]), чтобы лучше понять, каковы его ожидания от GNSO и ожидает ли он, что дальнейшая политическая работа будет способствовать (или нет) уже осуществляемым инициативам».
 - В [ответе GAC](#) (4 апреля 2022 года) на запрос GNSO мнения сообщества по формированию политики в области злоупотреблений DNS председатель GAC обратил внимание на важность этого «давно назревшего вопроса для GAC» и на заинтересованность GAC «в общественном обсуждении, работе и выработке общей позиции перед запуском новых gTLD». В свете того факта, что «работа сообщества может принести положительные инициативы и результаты, что может устранить необходимость в PDP», в письме было высказано предположение: «В данный момент [...] планирование действий PDP может быть преждевременным».
 - Наряду с другими ответами сообщества, ответ [Института по борьбе со злоупотреблениями DNS PIR](#) (22 апреля) был опубликован и получил [ответ генерального директора ICANN](#) (9 мая), в котором подчеркивалось «инновационное» предложение PIR «узкоспециализированных PDP», а также [Краткий обзор тенденций злоупотреблений DNS](#) от ICANN (22 марта).
- **Меры и инициативы регистратур и регистраторов по борьбе со злоупотреблениями DNS**
 - 27 марта 2020 года корпорация ICANN [внесла в соглашение об администрировании домена верхнего уровня .COM предложенную поправку](#), которая **расширяет действие договорных положений, способствующих обнаружению злоупотреблений DNS и информированию о них. Теперь такие положения**

охватывают две трети пространства имен gTLD⁶. Кроме того, в имеющем юридическую силу [договоре 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, и заинтересованные стороны, занимающиеся обеспечением общественной безопасности,** сообщили⁷ о своем сотрудничестве, которое призвано способствовать подготовке сообщений о злоупотреблениях, их рассмотрению и передаче в соответствующую юрисдикцию путем введения стандартной формы сообщения и создания единого контактного центра для соответствующих органов власти. В основу этих усилий легли рабочие отношения, установленные между правоохранительными органами и регистраторами, а также публикация **Группой заинтересованных сторон-регистраторов** в период проведения конференции ICANN67 документа [Порядок обращения к регистратору с жалобами на неправомерное использование доменов](#). Данное руководство было [обновлено](#) (январь 2022 г.) и одобрено **группой заинтересованных сторон-регистратур**.
- **Регистратура доменов общественного характера (PIR),** оператор регистратуры домена .ORG, и несколько новых gTLD [создали](#) (17 февраля 2021 года) **Институт по борьбе со злоупотреблениями DNS**. Для [PSWG GAC была проведена презентация](#) (3 марта 2021 года), посвященная этой инициативе. GAC в [Коммюнике по результатам заседаний на ICANN70](#) приветствовал создание Института по борьбе со злоупотреблениями DNS и «*приз[вал] сообщество объединить усилия для принятия комплексных мер, направленных на решение проблемы злоупотреблений DNS*». За прошедший период Институт по борьбе со злоупотреблениями DNS [выпустил Дорожную карту](#) (14 июня 2021 года), опубликовал [статью](#) (24 августа 2021 года), в которой рассматриваются меры по сокращению вреда на различных уровнях инфраструктуры интернета. Совсем недавно он сообщил о разработке [централизованного инструмента информирования о злоупотреблениях](#) или CART (18 ноября 2021 года), опубликовал [Передовые практики в сфере выявления злонамеренных регистраций](#) (2 декабря 2021 года) и отчет об инициативе CART, в котором она переименовывается в [NetBeacon](#) (4 апреля 2022 года).

⁶ К таким положениям относится [пункт 3b спецификации 11](#), действие которого до сих пор распространялось только на новые gTLD.

⁷ См. презентации сторон, связанных договорными обязательствами, [до](#) и [во время конференции ICANN68](#), а также [брифинг, проведенный PSWG для GAC](#) на ICANN68.

- **Многосторонний ответ корпорации ICANN⁸ (теперь часть программы по снижению угроз безопасности DNS) и обеспечение соблюдения договора**
 - Корпорация ICANN [представила](#) (22 июля 2021 года) свою [Программу по борьбе с угрозами безопасности DNS](#), которая призвана обеспечить прозрачность и ясность в отношении различных инициатив и проектов, связанных с угрозами безопасности DNS, а также дает возможность формировать и осуществлять централизованную стратегию.
 - **Офис технического директора ICANN (ОСТО) 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 форумах, посвященных анализу киберугроз и реагированию на инциденты, а также разрабатывает системы и инструменты для помощи в выявлении, анализе и предоставлении отчетности о злоупотреблениях DNS⁹.
 - В ответ на кризис COVID-19 ОСТО разработал инструмент **сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR)**, помогающий идентифицировать доменные имена, используемые для злоупотреблений, связанных с COVID-19, и делиться данными с соответствующими сторонами. Первоначально для GAC был [проведен брифинг](#) по этому вопросу перед началом ICANN68 (12 июня 2020 года), и членам GAC было предложено внести вклад в обеспечение языкового разнообразия данного инструмента.
 - Через свою **платформу отчетности о случаях злоупотребления доменами (DAAR)** ICANN с января 2018 года [ежемесячно публикует отчеты](#) о регистрации доменных имен и угрозах безопасности, наблюдаемых в DNS¹⁰. В октябре 2021 года корпорация ICANN и Группа заинтересованных сторон-регистратур сообщили о своем принципиальном согласии¹¹ использовать регистрационные данные, хранящиеся в регистратуре, для предоставления информации на уровне регистратора в DAAR, что было [признано GAC](#) в недавнем письме в ICANN (21 февраля 2022 года).

⁸ Генеральный директор ICANN опубликовал 20 апреля 2020 года заметку в блоге с подробным описанием [комплексного подхода корпорации ICANN к реагированию на злоупотребления DNS](#)

⁹ Во время [телеконференции GAC по вопросам злоупотреблений DNS](#) (24 февраля 2021 года) корпорация ICANN предоставила свежую информацию о деятельности ОСТО, связанной со злоупотреблениями DNS, в том числе состоялось обсуждение определений «угроза безопасности DNS» и «злоупотребление DNS», обязательств договорных сторон, платформы отчетности о случаях злоупотребления доменами (DAAR), инструмента сбора и регистрации информации об угрозах безопасности доменным именам (DNSTICR), состояния дел с инициативой по содействию безопасности системы доменных имен (DSFI) и новой инициативой по обмену знаниями и запуску стандартов для DNS и безопасности в области присвоения имен (KINDNS), а также была рассмотрена деятельность ОСТО в области обучения и наращивания потенциала во всем мире.

¹⁰ Некоторые заинтересованные стороны и участники инициатив ICANN прокомментировали ограничения DAAR, в частности в адресованном корпорации ICANN [письме](#) М3AAWG (5 апреля 2019 года) и в [проекте отчета](#) группы по анализу SSR2 (24 января 2020 года). Кроме того, Группа заинтересованных сторон-регистратур выразила свою озабоченность и дала рекомендации в [письме](#) техническому директору ICANN (9 сентября 2020 года).

¹¹ См. письмо RuSG в ICANN (22 октября 2021 года) и блог ICANN (28 октября 2021 года)

- ОСТО поддержал [организованную](#) в мае 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](#) с целью «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». Ее [Итоговый отчет](#) (15 октября 2021 года) был [опубликован](#) после 18 месяцев обсуждений. Корпорация ICANN [сообщила GAC](#) (16 февраля 2022 г.), что в настоящее время разрабатывает соответствующий план действий. 20 апреля 2022 года сообществу был представлен [процесс реализации](#) и [вики-страница](#) для отслеживания хода работы.
- **Что касается обеспечения соблюдения договорных обязательств**, в своей [заметке](#), опубликованной в 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, отдел соблюдения договорных обязательств ICANN в тесном контакте с офисом технического директора работает над определением угроз безопасности DNS [...] и сопоставлением этих угроз со спонсирующими сторонами, связанными договорными обязательствами. С помощью данных, собираемых в процессе проведения аудита [...], отдел соблюдения договорных обязательств ICANN оценивает то, насколько те или иные регистратуры и регистраторы соблюдают свои обязательства в части борьбы с угрозами безопасности DNS. Кроме данных, получаемых в процессе аудита, отдел соблюдения договорных обязательств ICANN использует также данные, полученные офисом технического директора и другими сторонами, для профилактической работы с регистратурами и регистраторами, ответственными за непропорционально большое количество угроз безопасности DNS. В тех случаях, когда конструктивное сотрудничество не приносит результата, отдел соблюдения договорных обязательств ICANN готов прибегать к решительным мерам принудительного исполнения обязательств в части защиты от угроз безопасности DNS в отношении тех, кто отказывается соблюдать их добровольно».*
 - После проведенного ранее **аудита соблюдения договорных обязательств** операторами регистратур, направленного на борьбу со злоупотреблениями в инфраструктуре DNS, который завершился в июне 2019 года¹², ICANN

¹² См. заметку в блоге ICANN [Контроль исполнения договорных обязательств: борьба со злоупотреблениями на уровне инфраструктуры системы доменных имен \(DNS\)](#) (8 ноября 2018 года) и [отчет отдела по контролю исполнения договорных обязательств по результатам проведения аудита мер по устранению угроз безопасности DNS, принимаемых операторами регистратур](#) (17 сентября 2019 года).

[опубликовала отчет](#) (24 августа 2021 года) о результатах **аудита соблюдения регистраторами обязательств в области злоупотреблений DNS**:

- проверено 126 регистраторов (под управлением которых находится более 90% всех зарегистрированных в gTLD доменов)
 - 111 регистраторов не полностью выполняют требования, связанные с получением и обработкой уведомлений о злоупотреблениях DNS (разделы 3.18.1–3.18.3 RAA)
 - 92 регистратора предприняли действия по обеспечению полного соответствия требованиям, 19 находятся на этапе внесения изменений
- 13 апреля 2022 года был [объявлен новый раунд аудита выбранных регистратур](#). Он затронет 28 операторов регистратур с gTLD, которые ранее не подвергались стандартному полномасштабному аудиту и имеют наивысшую оценку в области злоупотреблений согласно общедоступным репутационным блок-листам (за исключением спама). Ожидается, что аудит будет завершен до 3 квартала 2022 года.
- Во время [брифинга для GAC \(16 февраля 2022 г.\), организованного генеральным директором ICANN перед началом конференции ICANN73](#) (16 февраля 2022 года), специалисты отдела по контролю исполнения договорных обязательств ICANN рассмотрели обязательства в отношении злоупотреблений DNS, закрепленные в соглашениях ICANN, и представили результаты выборки из 3378 жалоб, касающихся обработки регистраторами сообщений о злоупотреблениях, что привело к 456 запросам о соблюдении требований и 1 уведомлению о нарушении.
- 9 марта 2022 года корпорация ICANN [объявила](#) о выпуске нового механизма информирования с улучшением отображения количества и тенденций жалоб.
- **Что касается тенденций злоупотреблений DNS**, корпорация ICANN провела анализ истории тенденций злоупотреблений DNS: [Анализ последних четырех лет: Краткий обзор тенденций злоупотреблений DNS](#) (22 марта 2022 года), на который ссылались в ходе вводного вебинара GAC на тему [Роль ICANN в создании и обеспечении исполнения глобальных политик DNS](#) (16 мая 2022 года).

Рекомендации сообщества по дальнейшей работе

- **Рекомендации по результатам проверки SSR2**

- Группа по анализу SSR2 представила [проект отчета](#) (24 января 2020 года), в котором сделан акцент на мерах по предотвращению и смягчению последствий злоупотреблений DNS. В своем [комментарии](#) (3 апреля 2020 года) GAC одобрил многие рекомендации, в том числе направленные на улучшение платформы отчетности о случаях злоупотребления доменами (DAAR) и укрепление механизмов контроля за соблюдением 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](#).
- Правление ICANN [предприняло действия](#) (22 июля 2021 года) по 63 итоговым рекомендациям группы по анализу (25 января 2021 года). В [блоге](#) корпорации ICANN резюмированы предпринятые действия:
 - 13 рекомендаций одобрены (находятся на этапе составления плана их выполнения),
 - 16 рекомендаций отклонены (в том числе 6 рекомендаций, которые не могут быть в полной мере одобрены),
 - 34 рекомендации отложены до проведения анализа и получения дополнительной информации.
- В [коммюнике по результатам заседаний Правительственного консультативного комитета на ICANN72](#) (1 ноября 2021 года) GAC рекомендовал Правлению ICANN:
 - *В приоритетном порядке предпринять последующие действия, необходимые для поддержки скорейшего выполнения оценочного отчета Правления [...] и*
 - *Предоставить дополнительную информацию о расхождении в интерпретации Правлением и группой по анализу SSR2 уровня выполнения некоторых рекомендаций.*
- Правление ICANN предоставило дополнительную информацию в своем [ответе](#) на Коммюнике ICANN72 (16 января 2022 года). Эту тему GAC и Правление ICANN обсуждали на ICANN73¹³. Также ей посвящены последующие обращения корпорации ICANN к GAC в [письме](#) (18 марта 2022 года) и [последующем электронном письме](#) (12 апреля 2022 года).
- **Рабочая группа Консультативного комитета по безопасности и стабильности (SSAC) по борьбе со злоупотреблениями DNS** опубликовала свой отчет — документ [SAC115](#) (19 марта 2021 года), в котором предлагается функционально совместимый подход к борьбе со злоупотреблениями в DNS.
 - **SSAC предложил общую концепцию передовых методов и процессов** для оптимизации отчетности о злоупотреблениях в DNS и интернете в целом. Рассмотрены следующие вопросы: основной центр ответственности за устранение злоупотреблений, стандарты доказывания, каналы передачи разрешения проблем

¹³ см. [протокол GAC на ICANN73](#), стр. 13

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 «координатора по реагированию 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 передачи данных (CDN), чтобы оптимизировать систему информирования о злоупотреблениях и свести к минимуму виктимизацию от злоупотреблений.
- Институт по борьбе со злоупотреблениями DNS сообщил о разработке [централизованного инструмента информирования о злоупотреблениях](#) (18 ноября 2021 года), о котором GAC сообщает в ходе ICANN74.

Важнейшие справочные документы

- [Ответ GAC на запрос GNSO мнения сообщества](#) по формированию политики в области злоупотреблений DNS (4 апреля 2022 года)
- [Анализ последних четырех лет: Краткий обзор по вопросам злоупотреблений DNS](#) (22 марта 2022 года)
- [Исследование Европейской комиссии о злоупотреблении DNS](#) и его [техническое приложение](#) (31 января 2022 г.)
- [Итоговый отчет](#) о проверке SSR2 (25 января 2021 года) и [оценочный отчет о действиях Правления](#) (22 июля 2021 года)
- [Объявление](#) ICANN и [отчет](#) (24 августа 2021 года) о результатах аудита соблюдения регистраторами обязательств в области злоупотреблений DNS.
- [Отчет SAC115](#) SSAC (19 марта 2021 года), предложение о функционально совместимом подходе к решению проблемы со злоупотреблениями в DNS.

Дальнейшая информация

Информационный документ GAC по политике в области борьбы со злоупотреблениями DNS
<https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf>

Управление документом

Название	Информационные материалы заседания GAC на ICANN74 — Борьба со злоупотреблениями DNS
Распространение	Члены GAC (до заседания) и общественность (после заседания)
Дата распространения	Версия 1: