

Борьба со злоупотреблениями DNS

Заседание 3

Содержание

Задача заседания	стр. 1	Предложение руководства по действиям GAC	стр. 1	Текущее положение дел и последние события	стр. 2	Важнейшие справочные документы	стр. 5
------------------	--------	--	--------	---	--------	--------------------------------	--------

Задачи заседания

Задача этого заседания — продолжить рассмотрение в GAC инициатив корпорации ICANN и сообщества ICANN по предотвращению и сокращению масштабов злоупотреблений DNS. Сюда относится выполнение рекомендаций по итогам проверок CCT и SSR2, дискуссии после завершения деятельности рабочей группы GNSO по PDP в отношении последующих процедур, применимых к новым gTLD, а также недавние предложения SSAC о создании координатора по реагированию на злоупотребления DNS. Это заседание также позволит продолжить обсуждение возможных конкретных предложений GAC.

Предложение руководства по действиям GAC

1. Рассмотреть [резолюцию](#) и [оценочный отчет](#) Правления ICANN (22 июля 2021 года) о действиях по рекомендациям [итогового отчета](#) (25 января 2021 года) второй группы по анализу и проверке безопасности, стабильности и отказоустойчивости DNS (SSR2). GAC направил свои [комментарии](#) касательно этих рекомендаций (8 апреля 2021 года)¹.
2. Рассмотреть результаты проведенного корпорацией ICANN аудита соблюдения регистраторами обязательств в области злоупотреблений DNS, представленные в [объявлении](#) и [отчете](#) (24 августа 2021 года).
3. Рассмотреть предложение SSAC по использованию [функционально совместимого подхода к борьбе со злоупотреблениями в DNS](#) (19 марта 2021 года), в том числе предложение создать «координатора по реагированию на злоупотребления» — независимую, неправительственную некоммерческую организацию, которая будет выступать в качестве

¹ См. также заметку в блоге корпорации ICANN [Решение Правления и дальнейшие действия в отношении проверки SSR2](#) (от 26 июля 2021 года), где приведена краткая информация об этом решении Правления.

координатора всей экосистемы DNS, чтобы оптимизировать систему информирования о злоупотреблениях и свести к минимуму виктимизацию от злоупотреблений.

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 DNS² 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 **регистрарам 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 ICANN³, в том числе пересмотр договоров ICANN с регистрарами 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.
- **Руководители GAC и Совет GNSO обсудили конкретные вопросы GAC**, которые передавались GNSO накануне каждой конференции ICANN, начиная с ICANN70⁴
 - **GAC запросил у GNSO свежую информацию о работе сообщества**, которую планируется провести в свете результатов PDP по процедурам для последующих раундов программы New gTLD (соответствующая рабочая группа воздержалась от рекомендаций по сокращению масштабов злоупотреблений DNS только для будущих новых gTLD), рекомендаций по итогам проверки SSR2 и рекомендаций SSAC, представленных в документе SAC115.
 - Как зафиксировано в протоколах заседаний GAC на конференциях [ICANN70](#) (стр. 16) и [ICANN71](#) (стр. 13), **руководители Совета GNSO признали важность этой темы для сообщества ICANN** и приняли во внимание длительное обсуждение этого вопроса, однако отметили, что **для продолжения работы необходимо определить соответствующий круг задач**, а также достигнуть **общего понимания**, в частности, в

² См. материалы соответствующих пленарных заседаний GAC на [ICANN66](#), [ICANN68](#), [ICANN69](#), [ICANN70](#) и [ICANN71](#).

³ 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](#).

⁴ См. [послания и вопросы Совету GNSO](#) накануне ICANN70

отношении определения понятия «злоупотребление DNS» и его совместимости с миссией ICANN.

- Что касается ожидаемых шагов со стороны GNSO, руководители Совета GNSO указали, что состоятся **консультации со сторонами, связанными договорными обязательствами, результатом которых может стать определение вариантов дальнейшей работы**. В соответствии с [реестром задач и решений Совета GNSO](#) (по состоянию на 23 сентября 2021 года) *«следующие шаги, касающиеся злоупотреблений DNS, если таковые требуются»*, еще предстоит определить.
- **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 gTLD⁵**. 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**, сообщили⁶ 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](#).
 - **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

⁵ К таким положениям относится [пункт 3b спецификации 11](#), действие которого до сих пор распространялось только на новые gTLD.

⁶ См. презентации сторон, связанных договорными обязательствами, [до](#) и [во время конференции ICANN68](#), а также [брифинг, проведенный PSWG для GAC](#) на ICANN68.

2021 года) и опубликовал [статью](#) (24 августа 2021 года), в которой рассматриваются меры по сокращению вреда на различных уровнях инфраструктуры интернета.

- **Комплексный подход корпорации ICANN к реагированию⁷ и обеспечение исполнения договорных обязательств**
 - **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 DNS⁸.
 - 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. Для GAC был [проведен брифинг](#) по этому вопросу перед началом ICANN68 (12 июня 2020 года), и членам комитета 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 DNS⁹.
 - ОСТО поддерживает [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». Отчет о ходе работ был представлен на [4-м симпозиуме DNS](#) (24 мая 2021 года) и ожидается [накануне ICANN72](#).

⁷ Генеральный директор ICANN опубликовал 20 апреля 2020 года заметку в блоге с подробным описанием [комплексного подхода корпорации ICANN к реагированию на злоупотребления DNS](#)

⁸ 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.

⁹ Некоторые заинтересованные стороны и участники инициатив ICANN прокомментировали ограничения DAAR, в частности в адресованном корпорации ICANN [письме](#) M3AAWG (5 апреля 2019 года) и в [проекте отчета](#) группы по анализу SSR2 (24 января 2020 года). Кроме того, Группа заинтересованных сторон-регистраторов выразила свою озабоченность и дала рекомендации в [письме](#) техническому директору ICANN (9 сентября 2020 года).

- **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.*

Эта заметка в блоге также дает представление об объемах жалоб, ресурсах, выделенных на их обработку, и статистике рассмотрения этих жалоб¹⁰.

- После проведенного ранее **аудита соблюдения договорных обязательств** операторами регистратур, направленного на борьбу со злоупотреблениями в инфраструктуре DNS, который завершился в июне 2019 года¹¹, ICANN [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
- Корпорация ICANN [представила](#) (22 июля 2021 года) свою [Программу по борьбе с](#)

¹⁰ Регулярная отчетность отдела по контролю исполнения договорных обязательств находится здесь: <https://www.icann.org/resources/compliance-reporting-performance>

¹¹ 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).

[угрозами безопасности DNS](#), которая призвана обеспечить прозрачность и ясность в отношении различных инициатив и проектов корпорации, связанных с угрозами безопасности DNS, а также дает возможность формировать и осуществлять централизованную стратегию.

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 соответствующей заметке в [блоге](#) корпорации ICANN виды этих действий сгруппированы следующим образом:
 - 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.

● 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.

- В указанном отчете **SSAC предложил общую концепцию передовых методов и процессов** для оптимизации отчетности о злоупотреблениях в DNS и 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 «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.

Важнейшие справочные документы

- [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.

Дополнительная 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 ICANN72 — Борьба со злоупотреблениями DNS
Распространение	Члены GAC (до заседания) и общественность (после заседания)
Дата распространения	Версия 1: 22 сентября 2021 года