ICANN | GAC

Governmental Advisory Committee

Распространение	Для общего доступа
Дата	18 сентября 2019 года

Заявление GAC о злоупотреблении DNS

Правительственный консультативный комитет ICANN (GAC) рад возможности принять участие в предстоящей сквозной дискуссии относительно злоупотребления DNS на конференции ICANN66 и выражает поддержку открытому письму сообществу на эту тему от группы заинтересованных сторон-регистратур от 19 августа 2019 года.

Защита общества от угроз безопасности и злоупотребления DNS является важным аспектом общественной политики. GAC публиковал рекомендации, предоставлял указания и комментарии, организовал сквозные дискуссии сообщества и выступал за более строгие контрактные обязательства по защите общества.[1] Наши текущие замечания помогают раскрыть эту тему путем обсуждения следующих вопросов: 1) почему злоупотребление DNS является жизненно важной темой; 2) имеющиеся определения и договорные обязательства касательно злоупотребления DNS; и 3) выводы и рекомендации Группы по анализу конкуренции, потребительского доверия и потребительского выбора касательно злоупотребления DNS. В ходе этой дискуссии мы надеемся заложить основу для продуктивной и информированной сквозной дискуссии сообщества в Монреале.

Почему злоупотребление DNS является насущной темой

С каждым годом затраты на борьбу с киберпреступностью во всем мире растут. В 2018 году по оценкам они достигли $600 млрд.[2] Для реализации своих планов киберпреступники используют слабые места системы DNS,[3] и самым распространенным средством первоначальной атаки является электронная почта,[4] что обусловило резкое увеличение количества фишинговых атак на потребителей.[5]

[1] GAC предоставил эти тезисы независимо и с трибуны Рабочей группы по обеспечению общественной безопасности. *См.* следующее: Коммюнике GAC: ICANN46 Пекин; ICANN53 Буэнос-Айрес, ICANN54 Дублин и ICANN57 Хайдарабад; доклады сообщества ICANN о злоупотреблении DNS в ходе ICANN57, 58 и 60; и рекомендации правоохранительных органов за 2009 год, одобренные GAC во время ICANN38).

[2] McAfee «Влияние киберпреступности на экономику — без остановки» (Economic Impact of Cybercrime – No Slowing Down) по адресу: https://www.csis.org/analysis/economic-impact-cybercrime; Accenture 2019 «Стоимость киберпреступности» (Cost of Cybercrime) по адресу https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

[3] *См. напр.* Symantec «Отчет о безопасности интернета» (Internet Threat Security Report) (февраль 2019 года) по адресу: https://www.symantec.com/security-center/threat-report.

[4] Verizon 2019 «Отчет о расследованиях утечек данных» (Data Breach Investigations Report) по адресу https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations- report.pdf

[5] Akamai 2019 «Обзор интернета» (State of the Internet) по адресу https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial- services-attack-economy-report-2019.pdf

Если общество полагается на интернет при общении и совершении финансовых операций, организации, заведующие инфраструктурой DNS, должны принять меры по обеспечению безопасности этого общественного ресурса. Недавно введенное законодательство о конфиденциальности личных данных, включая Общие положения о защите данных ЕС, ограничило доступ общества к информации о владельцах доменных имен, что осложняет задачу правоохранительным органам и специалистам по кибербезопасности, задачей которых является борьба с угрозами безопасности интернета.[6]
Недавние и текущие проверки ICANN, проводимые согласно Уставу, выявляют важность следующих факторов:

- эффективность **мер безопасности при решении реальных и потенциальных задач и угроз безопасности и стабильности DNS и степени надежности мер по обеспечению безопасности при решении будущих задач** и угроз безопасности;[7]
- **защита потребителей**, безопасности, стабильности и отказоустойчивости, **злоумышленных нарушений**, суверенитета и защиты прав до или во время выдачи разрешения на увеличение количества новых доменов верхнего уровня;[8]
- **повышение точности и доступности регистрационных данных в пространстве доменов общего пользования верхнего уровня**, а также мер защиты таких данных;[9]
- **эффективность** действующей на тот момент **службы каталогов регистратур gTLD** и того, **отвечает ли ее функционирование потребностям правоохранительных органов, укрепления потребительского доверия** и обеспечения сохранности данных владельцев доменов[10] [подчеркивание добавлено]

Также ICANN определяет особенности проведения следующего раунда ввода gTLD, что предоставляет новые возможности для включения в договоры поощрений за использование передовых практик для борьбы с таким злоупотреблением и увеличения стоимости ведения бизнеса при злоупотреблении или противоправных действиях.

Следовательно, сейчас следует рассмотреть эти вопросы и выбрать наилучший курс действий в поддержку обязательств ICANN поддерживать **и совершенствовать** систему управления DNS и «операционную стабильность, надежность, безопасность, глобальную функциональную совместимость, отказоустойчивость и открытость DNS и интернета».[11]
В этом отношении наиболее ценные данные могут предоставить правительства и государственные органы.[12]

[6] *См. напр.* Опрос пользователей GDPR и WHOIS ICANN, проведенный рабочей группой по вопросам борьбы с фишингом и рабочей группой по противодействию компьютерным злоумышленникам в области передачи сообщений, доступный по адресу https://www.securityskeptic.com/2019/03/facts-figures-whois-policy-changes-impair-blacklisting-defenses.html

[7] Устав ICANN, §4.6 (c), Анализ безопасности, стабильности и отказоустойчивости.

[8] Устав ICANN, §4.6 (d), Анализ конкуренции, потребительского доверия и потребительского выбора.

[9] Устав ICANN, §4.6 (e), Анализ службы каталогов регистрационных данных.

[10] *Там же*.

[11] Устав ICANN, §1.2(a) Обязательства.

[12] Признание жизненно важного вклада правительств и государственных органов в рассмотрение проблем общественной политики является одной из основных ценностей ICANN. Устав ICANN, §1.2(b) Основные ценности.

ICANN | GAC
Governmental Advisory Committee

Действующие определения понятий «злоупотребление DNS» и «договорные обязательства ICANN»

Группа по анализу конкуренции, потребительского доверия и потребительского выбора (CCT), состоящая из заинтересованных сторон сообщества ICANN, рассмотрела действующие в сообществе ICANN определения злоупотребления DNS, когда занималась оценкой ситуации со злоупотреблением DNS в новых gTLD по сравнению с историческими gTLD и оценкой эффективности имеющихся защитных мер.[13] Отметив, что, по данным сообщества ICANN, «существует консенсус по поводу определения злоупотребления безопасностью DNS или злоупотребления безопасностью инфраструктуры DNS», **группа по анализу CCT определила злоупотребление DNS как «умышленное введение в заблуждение, попустительство или нежелательную деятельность с активным использованием DNS и/или процедур регистрации доменных имен».**[14] В отчете CCT термин «злоупотребление безопасностью DNS» относится к техническим сторонам злонамеренных действий, таким как вредоносное ПО, фишинг и ботнеты, а также спам в случае использования в качестве средства доставки для вышеуказанного.[15]

Эти определения соответствуют таковым в стандартных договорах ICANN для регистратур и регистраторов. Стандартное Соглашение об администрировании домена верхнего уровня ICANN содержало требование к операторам регистратур новых gTLD включать в их Соглашения между регистратурами и регистраторами (RRA) положения, которые накладывают на владельцев доменов следующие запреты:

> распространять вредоносное ПО, принимать участие в злоупотреблениях с использованием ботнетов, 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 (соответствующие законодательству и любым сопряженным процедурам) такой деятельности, в том числе приостановка регистрации доменного имени.[16]

Также 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».[17][подчеркивание добавлено]. Данный перечень приведен для ознакомления и не является полным. В дополнение к условиям для регистратур, стандартный договор ICANN для регистраторов требует от них «расследования и надлежащего реагирования на любые сообщения о злоупотреблениях».[18] Вместе эти источники, разработанные в сообществе многих заинтересованных сторон ICANN, образуют общее основополагающее определение злоупотребления DNS.

---

[13] *См.* Итоговый отчет CCT (18 сентября 2018 года) на стр. 88-109.Чтобы получить дополнительные сведения о том, как злоупотребления характеризуются сообществом ICANN, см. итоговый отчет Рабочей группы по политике в сфере противодействия злоупотреблениям при регистрации (29 мая 2010 года), https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf

[14] Итоговый отчет CCT на стр. 88 и сопроводительные материалы. *См. также* стр. 3 «Меры защиты от злоупотребления DNS, предусмотренные в составе Программы New gTLD:Пересмотренный отчет» (2016 год).

[15] Итоговый отчет CCT на стр. 8.

[16] ICANN, Соглашение об администрировании домена верхнего уровня, спецификация 11, 3(a).

[17] ICANN, Соглашение об администрировании домена верхнего уровня, спецификация 11, 3(b). Это положение часто фигурировало в вопросах и рекомендациях GAC, которые возникали из-за того, что реализация этого средства защиты со стороны ICANN на фоне требований к регистратурам следить за угрозами безопасности не требовала от операторов регистратур реагировать на угрозы безопасности. *См.* Сингапур (2014), Лос-Анджелес, Лондон. В пекинском коммюнике GAC была указана обязанность не только следить за появлением угроз безопасности, но и реагировать в случае обнаружения определенных приоритетных угроз безопасности. Комитет GAC рекомендовал, чтобы в случае выявления угроз безопасности, создающих «риск реального ущерба», оператор регистратуры ставил в известность соответствующего регистратора и, если регистратор не примет «незамедлительных мер», «приостанавливать регистрацию доменного имени до решения соответствующего вопроса». Пекинское коммюнике на стр. 7.

[18] ICANN, Соглашение об аккредитации регистраторов, § 3.18.

ICANN | GAC
Governmental Advisory Committee

Группа по анализу CCT выявляет сосредоточение злоупотреблений DNS вокруг отдельных регистратур и регистраторов и вырабатывает рекомендации

Группа по анализу CCT определила, что доменные имена зачастую становятся ключевым компонентом киберпреступности и используются для распространения вредоносного ПО и управления ботнетами. Кампании рассылки спама зачастую демонстрируют корреляцию с фишингом и другими видами киберпреступности.[19] В частности, группа по анализу указала следующее:

> Хотя в типовых договорах ICANN с регистратурами и регистраторами предусмотрено обязательное использование конкретных мер защиты, усилия по борьбе со злоупотреблениями при использовании доменных имен существенно разнятся среди сторон, связанных договорными обязательствами. Некоторые организации бездействуют до получения жалобы. Другие регистраторы, наоборот, предпринимают активные действия, такие как проверка идентификационных данных владельцев доменов, блокирование строк доменных имен, похожих на известные цели фишинговых атак, и тщательная проверка реселлеров доменных имен. Реселлеры доменных имен не связаны с ICANN договорными обязательствами. Следовательно, ICANN не может напрямую контролировать соблюдение ими стандартных контрактных требований. . . [20]

Для лучшего понимания эффективности мер защиты новых gTLD группа по анализу CCT заказала проведение анализа уровней распространения спама, фишинга и вредоносного ПО в глобальных gTLD с 2014 по 2016 годы с разделением между историческими и новыми gTLD и опубликовала соответствующий отчет.[21] Исследование злоупотребления DNS обращает внимание на то, что существуют серьезные проблемы со злоупотреблением DNS. Касательно программы новых gTLD, исследование отмечает, что более 50% регистраций отдельных новых gTLD имели характер злоупотреблений.[22] Также в исследовании отмечено следующее:

- Новые gTLD стали более заметной целью для злоумышленников;
- Среди исторических gTLD доля скомпрометированных доменов выше, при этом злоумышленники часто предпочитают регистрировать доменные имена с использованием новых gTLD;
- Наибольшее количество злоупотреблений отмечается по тем регистратурам новых gTLD, операторы которых участвуют в ценовой конкуренции;
- Со временем уровни злоупотреблений путем фишинга и вредоносного ПО с использованием новых gTLD достигают показателей исторических gTLD;
- К пяти новым gTLD с наибольшей концентрацией доменов, задействованных в фишинговых атаках, согласно черному списку Антифишинговой рабочей группы, относилось 58,7% всех доменов из черного списка новых gTLD;
- В последний квартал 2016 года отмечен существенно больший процент спама с использованием новых gTLD, чем с использованием исторических gTLD (в десять раз больше, чем для исторических gTLD);

[19] Итоговый отчет CCT на стр. 93.
[20] Итоговый отчет CCT на стр. 93.
[21] *См.* https://www.icann.org/news/announcement-2017-08-09-en.
[22] Итоговый отчет о статистическом анализе злоупотреблений DNS в gTLD (9 августа 2017 года): https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

- Зарегистрированные со злонамеренными целями доменные имена часто содержат строки, связанные с товарными знаками
- Количество злоупотреблений обычно связано со строгостью требований для регистрации: *например*, злоумышленники предпочитают регистрировать домены в стандартных новых gTLD, обычно открытых для публичной регистрации имен, а не в новых gTLD сообществ, ограничивающих круг лиц, которым разрешена регистрация доменных имен.

Группа по анализу CCT пришла к выводу, что на объемы злоупотреблений влияют такие факторы, как регистрационные ограничения, цена и практические методы работы конкретных регистраторов.[23] Как следствие, группа по анализу CCT дала следующие рекомендации:

- Корпорация ICANN должна согласовать с регистратурами поправки к действующим соглашениям об администрировании доменов верхнего уровня или условия новых соглашений об администрировании доменов верхнего уровня для будущих раундов создания новых gTLD, **чтобы включить в эти соглашения ряд стимулов, в том числе финансовых, для принятия регистратурами, особенно с политикой открытой регистрации, активных мер борьбы со злоупотреблениями.**[подчеркивание добавлено];
- Корпорации ICANN следует обсудить поправки к соглашению об аккредитации регистраторов и соглашениям об администрировании доменов верхнего уровня для включения положений, направленных на предотвращение систематического использования конкретных регистраторов или регистратур для злоупотреблений в области безопасности DNS. В частности, ICANN следует установить пороговые значения объемов злоупотреблений, при которых будет происходить автоматическая отправка уведомлений отделом по контролю исполнения договорных обязательств, и более высокий порог, при достижении которого регистраторы и регистратуры будут считаться нарушившими свои обязательства по соглашениям;
- Дополнительно изучить взаимосвязь между конкретными операторами регистратур, регистраторами и злоупотреблениями в области безопасности DNS, заказав постоянный сбор данных, в том числе в рамках инициатив платформы отчетности о случаях злоупотребления доменами (DAAR) ICANN. Для обеспечения транспарентности эта информация должна регулярно публиковаться, в идеальном случае ежеквартально, но не реже одного раза в год, позволяя выявить регистратуры и регистраторов, которых корпорация ICANN должна строже контролировать, проверять и, возможно, принуждать к соблюдению обязательств. При обнаружении признаков злоупотреблений ICANN должна составить план действий, чтобы отреагировать на результаты таких исследований, устранить выявленные проблемы и определить категории данных для постоянного сбора в будущем; и
- ICANN должна собрать и опубликовать данные о цепочке сторон, отвечающих за регистрацию доменных имен в gTLD.

[23] Итоговый отчет CCT на стр. 94, касательно исследования злоупотребления DNS, стр. 24-25.

Передовой опыт регистратур ccTLD

В последние годы все большее количество регистратур ccTLD использует активные меры для защиты от злоупотреблений с целью борьбы с преступлениями, связанными с DNS, очистки их зон от злоупотреблений и борьбы со злоумышленниками за счет уменьшения привлекательности для них своих доменных имен. Среди этих мер более надежные методы проверки подлинности, методы проверки личности, [24] использование моделей прогнозирования мошенничества, основанных на данных регистрации и инфраструктуры, для выявления и прогнозирования регистрации доменов в незаконных целях. [25] Эти проверенные передовые методы необходимо внедрить регистратурам и регистраторам gTLD.

Заключение

Сообщество имеет уникальную возможность оценить и выбрать политики, необходимые для защиты общества от злоупотребления DNS. Мы соглашаемся с группой заинтересованных сторон-регистратур в том, что успех их работы (и самой системы DNS) зависит от их возможности предложить продукт, которому пользователи смогут доверять. Чтобы эффективнее бороться со злоупотреблением DNS и создать более достойную доверия систему DNS, мы призываем сообщество серьезно задуматься над выполнением вышеуказанных рекомендаций, так как они представляют собой действенные меры, которые можно *и нужно* принять для борьбы со злоупотреблением DNS. GAC ожидает возможности обсудить эту тему с другими группами сообщества на ICANN66 в Монреале.

[24] Например, см. Заседание ICANN64 по выводам: Успех борьбы со злоупотреблением DNS в зоне .DK и https://www.dk-hostmaster.dk/en/news/mandatory- identification-nemid и https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

[25] См. https://eurid.eu/en/news/identification-of-malicious-dns/