

SAC 050

**Блокирование DNS: сравнение пользы и вреда —
заключение Консультативного комитета по
безопасности и стабильности по вопросу
блокирования доменов верхнего уровня в системе
доменных имен**



**Заключение Консультативного комитета
по безопасности и
стабильности (ККБС)
ICANN
14 июня 2011 г.**

Введение

Настоящий документ является заключением Консультативного комитета по безопасности и стабильности (ККБС). ККБС консультирует сообщество и Правление ICANN по вопросам, связанным с безопасностью и целостностью систем распределения имен и адресов Интернета. Сюда относятся эксплуатационные вопросы (например, имеющие отношение к правильной и надежной работе корневой системы имен), административные вопросы (например, имеющие отношение к распределению и назначению адресов Интернета) и регистрационные вопросы (например, имеющие отношение к услугам реестров и регистраторов). ККБС занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и адресов Интернета с целью определения источников основных угроз стабильности и безопасности, и предоставляет соответствующие рекомендации сообществу ICANN. ККБС не обладает полномочиями регламентировать, обеспечивать соблюдение или выносить решения по спорам. Эти функции принадлежат другим органам, и содержащиеся в настоящем документе сведения и должны рассматриваться по существу дела.

Имена авторов этого заключения, ссылки на биографии членов комитета и заявления о заинтересованности, а также возражения членов комитета, касающиеся выводов или рекомендаций, содержатся в конце настоящего документа.

Содержание

1. Блокирование DNS: сравнение пользы и вреда	4
2. Благодарности, заявления о заинтересованности, возражения и отказы от участия	6
2.1 Благодарности	6
2.2 Заявления о заинтересованности	7
2.3 Возражения и отказы от участия	7

1. Блокирование DNS: сравнение пользы и вреда

Блокирование или изменение ответов на запросы к системе доменных имен (DNS) приобретает все более заметные масштабы. Фильтрация доменных имен или адресов интернет-протокола (IP-адресов) (или создание в рамках политики обеспечения безопасности иных препятствий при доступе к веб-содержимому), возможно, рассматривается некоторыми организациями как естественное расширение существовавших ранее элементов контроля над телефонной связью, нацеленных на предотвращение оплаты междугородных телефонных разговоров сотрудников организации.

Технические решения по блокированию DNS нацелены на пользователей конкретного административного домена, например, частной или находящейся под управлением государства сети. Предотвращение разрешения доменного имени в IP-адрес будет препятствовать прямому соединению с поименованным узлом, хотя обходные технические методы могут так или иначе обеспечить возможность подключения к целевой системе (сюда относится просто доступ к сайту через IP-адрес вместо полного доменного имени (FQDN)). Распознаватель DNS или оператор сети также может переопределить ответ DNS таким образом, чтобы он содержал выбранный оператором IP-адрес, переопределив либо ответ о несуществующем домене (NXDOMAIN) или ответ DNS для существующего имени FQDN, с потенциально неблагоприятными последствиями для серверов имен с поддержкой расширений безопасности DNS (DNSSEC) и их пользователей. Наиболее грубым подходом со стороны оператора является отклонение запросов DNS без отправки ответа, хотя это приводит к недетерминированному поведению и само по себе способно создать проблемы.

Независимо от используемого механизма, организации, внедряющие блокирование, должны также применять следующие принципы:

1. Организация реализует политику по отношению к сети и ее пользователям, находящимся под административным контролем этой организации (т.е. она является администратором домена, подпадающего под действие политики).
2. Организация считает, что данная политика полезна для реализации задач организации и/или интересов ее пользователей.
3. Организация осуществляет реализацию данной политики с использованием метода, приносящего наименьший вред функционированию ее сети и пользователям, за исключением случаев, когда конкретные методы предписаны законами или нормативными актами.

4. Организация прилагает скоординированные усилия для предотвращения вреда для пользователей за пределами домена, в котором реализуется данная политика, вследствие внедрения этой политики.

Если эти принципы не будут применяться, блокирование использования DNS может причинить существенно больший косвенный ущерб или привести к непредвиденным последствиям в отсутствие средств защиты заинтересованных сторон.

Эволюция технологии Интернета основана на применении основополагающего принципа практической медицины — *primum no nocere* (Не навреди!) — требующего от медицинских работников учитывать возможный вред в результате их вмешательства. В случае блокирования DNS, независимо от того, применяется ли блокирование по отношению к доменам верхнего уровня (ДВУ) (например, .example) или второго (например, example.example) и третьего уровня (например, example.example.example), «непричинение вреда» означает недопустимость обстоятельств, в которых будет оказано отрицательное влияние на пользователей Интернета, находящихся за пределами действия политики организации в отношении доменов, в результате реализации этой политики.

Любые технические подходы к блокированию DNS и, в еще большей степени, попытки обхода блокирования окажут некоторое влияние на безопасность и/или стабильность работы пользователей и приложений, а также на когерентность или универсальность разрешения в мировом пространстве имен. ККБС не может провести черту между «хорошим блокированием DNS» и «плохим блокированием DNS» на любом уровне ДВУ, хотя Комитет может предложить проведение исследования наблюдаемых последствий различных подходов к блокированию и по его результатам сформулировать руководящие принципы для использования при оценке того, какие подходы к блокированию, скорее всего, приведут к наименьшему количеству непреднамеренных последствий и наименьшему вреду за пределами блокируемого домена. Например, отрицательные последствия блокирования DNS на уровне конкретных доменов или имен узлов для безопасности DNS описаны в недавно опубликованном информационном документе.¹

ККБС осознает, что тема блокирования DNS была поднята в связи с добавлением в корневую зону родового ДВУ (рДВУ) XXX. ККБС не располагает достаточной информацией, чтобы занять определенную позицию в отношении данного действия, однако Комитет желает разъяснить, что, независимо от того, применяется ли блокирование на уровне ДВУ или на подуровнях, для минимизации вреда требуются согласованные усилия по предотвращению возникновения обстоятельств, когда в результате реализации политики блокирования будет оказано отрицательное влияние на пользователей Интернета, находящихся за

¹ См. <http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf>.

пределами домена, в котором организация реализует свою политику. Расширение этой нравственной концепции уровня организаций на суверенные государства потребует более глубокого понимания политической ситуации, чем то, которым в настоящее время обладает ККБС. Но мы также с определенностью можем заявить, что блокирование целых ДВУ на уровне стран создает фундаментальные препятствия для выполнения задачи предоставления единой, унифицированной системы имен для ресурсов Интернета. В случае реализации без применения некоторых официальных этических рамок для минимизации вреда внешним сторонам, блокирование может оказать более сильное отрицательное влияние на широкие сообщества, чем ожидается, усугубляя проблемы, которые такое блокирование должно было решить. Кроме того, блокирование на втором и третьем уровне доменов, так же как и на уровне ДВУ, может дать толчок развитию альтернативных систем имен и/или корневых зон, что окажет дестабилизирующее и разрушающее влияние на Интернет.

2. Благодарности, заявления о заинтересованности, возражения и отказы от участия

В этих разделах читателю предоставляется информация по трем аспектам нашего процесса. В разделе «Благодарности» перечислены участники, которые внесли свой вклад в подготовку настоящего документа. В разделе «Заявления о заинтересованности» содержатся ссылки на биографии членов Комитета и любые конфликты интересов (фактические, кажущиеся или потенциальные), которые могут отразиться на материалах настоящего документа. Раздел «Возражения и отказы от участия» предоставляет возможность отдельным членам выразить свое несогласие с содержанием настоящего документа или процессом его подготовки.

2.1 Благодарности

Комитет выражает свою благодарность следующим членам ККБС и другим лицам, внесшим свой вклад, за потраченное время, усилия и анализ, выполненный при подготовке настоящего отчета.

КС Клэффи (KC Claffy)
Стив Крокер (Steve Crocker)
Патрик Фальтстром (Patrik Fältström)
Джим Гэлвин (Jim Galvin)
Уоррен Кумэри (Warren Kumari)
Джейсон Ливингуд (Jason Livingood)
Дэнни Макферсон (Danny McPherson)
Рэм Мохан (Ram Mohan)
Дейв Пичителло (Dave Piscitello)
Брюс Тонкин (Bruce Tonkin)
Пол Вокси (Paul Vixie)

2.2 Заявления о заинтересованности

Биографические сведения о членах ККБС и заявления о заинтересованности доступны по адресу:

<http://www.icann.org/en/committees/security/biographies-25mar11-en.htm>.

2.3 Возражения и отказы от участия

Возражений и отказов от участия не поступило.