Квантовые вычисления и DNS

Офис технического директора ICANN

Пол Хофман (Paul Hoffman)
OCTO-031
11 февраля 2022 г.

СОДЕРЖАНИЕ

ОСНОВНЫЕ ПОЛОЖЕНИЯ 3

1 ВВЕДЕНИЕ 3

Настоящий документ входит в серию документов офиса технического директора ICANN (OCTO). Список документов этой серии см. на странице публикаций OCTO. Вопросы или предложения по любому из этих документов принимаются по адресу octo@icann.org.

Настоящий документ составлен в поддержку стратегической задачи ICANN — повысить общую ответственность за обеспечение безопасности и стабильности системы доменных имен (DNS) за счет укрепления координации DNS в партнерстве с соответствующими заинтересованными сторонами. Это часть стратегической цели ICANN по укреплению безопасности DNS и системы корневых серверов DNS (RSS).

Основные положения

В последние годы внимание специалистов по безопасности привлекли квантовые компьютеры, поскольку существует возможность того, что они способны подорвать повсеместно используемые ныне криптографические алгоритмы. Пока достаточно мощных для этого квантовых компьютеров не существует, однако по мере развития технологий может наступить день, когда некоторые из используемых сегодня алгоритмов можно будет с легкостью взломать при помощи компьютеров этого нового типа. Вместе с тем, поскольку технология квантовых вычислений по-прежнему является новой, а создание и эксплуатация квантовых компьютеров стоят очень дорого, трудно спрогнозировать, когда в обозримом будущем наступит этот день.

В настоящее время идет стандартизация новых алгоритмов, которые, как предполагается, будут неуязвимыми для квантовых компьютеров. В данной статье рассматривается недавно проделанная работа, позволяющая сделать более точные прогнозы относительно того, в каких ситуациях сообществу системы доменных имен (DNS) надо будет рассматривать возможность перехода от существующих криптографических алгоритмов к новым.

1 Введение

В современной криптографии некоторые алгоритмы зависят от сложности определенных математических задач, решение которых занимает огромное количество времени. Квантовые компьютеры смогут решать эти задачи гораздо быстрее, что ослабит гарантии, обеспечиваемыми этими алгоритмами. Компьютеры, основанные на принципах квантовой механики, коренным образом отличаются от компьютеров, широко использующихся последние 70 лет. Обработка данных при помощи квантовых компьютеров основана не на двоичных битах, которые сегодня используются во всех компьютерах, а на квантовых битах, получивших название *кубиты*.

Если удастся создать большие квантовые компьютеры, они, возможно, позволят решить некоторые задачи, не поддающиеся решению современными вычислительными технологиями, поскольку квантовые компьютеры способны выполнять множество сложных процессов одновременно. Хотя современные компьютеры, известные как *классические*, способны выполнять параллельные процессы, квантовые компьютеры делают это за счет использования более тесных связей между разными частями анализируемых данных.

Концепции, на которых основаны квантовые компьютеры, разрабатывались в течение почти 50 лет, однако создать даже очень маленькие квантовые компьютеры — дело необычайно сложное. Кубиты содержат достаточно хрупкую информацию, поэтому во время вычислительных операций их необходимо полностью изолировать от внешней среды, поддерживая температуру около нуля градусов по Кельвину; для этого требуется много оборудования и большое физическое пространство. Тем не менее, вероятность ошибок при обработке данных с использованием кубитов также весьма высока. Квантовому компьютеру нужны сотни или тысячи дополнительных охлаждаемых кубитов для исправления ошибок в вычислениях по каждому кубиту, и создание квантового

компьютера с миллионами кубитов может оказаться невозможным в связи с требованиями, предъявляемыми к охлаждению и связи.