Краткое руководство:
Подготовьте свои системы к обновлению KSK корневой зоны

Что такое обновление KSK корневой зоны?

Интернет-корпорация по присвоению имен и номеров (ICANN) планирует обновить (изменить) «верхнюю» пару криптографических ключей, используемых в протоколе расширений безопасности системы доменных имен (DNSSEC). Этот ключ обычно называют «ключом для подписания ключей (KSK) корневой зоны». Это будет первое изменение KSK с момента его генерирования в 2010 году. Это важный шаг в повышении безопасности, точно так же как регулярное изменение паролей считается правильным для каждого пользователя интернета.

Изменение ключа подразумевает генерирование новой пары криптографических ключей и распространение нового открытого компонента среди распознавателей, осуществляющих проверку DNSSEC. Это будет значительным изменением, поскольку при проверке пункта назначения с использованием DNSSEC каждый запрос в интернете зависит от KSK корневой зоны. Когда новые ключи будут сгенерированы, операторам, таким как интернет-провайдеры (ISP), понадобится обновить свои системы, перейдя к новому ключу, чтобы при попытке посещения веб-сайта ключ пользователя мог пройти проверку на соответствие новому KSK.

Почему необходимо подготовиться

В настоящее время около четверти пользователей интернета во всем мире заходят в интернет с использованием распознавателей с функцией проверки DNSSEC, которые могут быть затронуты обновлением ключа KSK. Если у таких распознавателей не будет нового ключа на момент обновления KSK, конечные пользователи, зависящие от работы этих распознавателей, столкнутся с ошибками и не смогут получить доступ к интернету.

Если вы не используете DNSSEC, то вашу систему обновление ключа не затронет. Однако следует иметь в виду, что DNSSEC является важным элементом предотвращения перехвата доменных имен.

ICANN предлагает операторам и другим заинтересованным сторонам испытательную площадку, позволяющую убедиться в готовности систем к процессу автоматизированного обновления. Проверьте готовность своих систем, перейдя по следующему адресу: **https://go.icann.org/KSKtest**.

Если у вас включена проверка DNSSEC, необходимо обновить свои системы, перейдя к новому KSK, чтобы обеспечить пользователям беспроблемный доступ к интернету.

Designed by ICANN Communications | март 2018 года

Что необходимо сделать

Свои системы можно обновить в любое время перед обновлением ключа с использованием нового KSK корневой зоны, опубликованного 11 июля 2017 года, и у некоторых, возможно, уже функционирует автоматическое обновление. Действия, которые нужно предпринять, зависят от следующего.

Если ваше программное обеспечение поддерживает автоматическое обновление якорей доверия DNSSEC (RFC 5011):

KSK должен быть обновлен автоматически в надлежащее время. Дополнительных действий с вашей стороны не требуется.

Обратите внимание, что устройства, которые во время обновления ключа не подключены к интернету, необходимо будет обновить вручную, если они будут подключены после завершения обновления.

Начиная с марта 2017 года ICANN предлагает операторам и другим заинтересованным сторонам испытательную площадку, с помощью которой можно проверить готовность своих систем к корректному проведению автоматизированного процесса обновления. Дополнительная информация находится по адресу **https://icann.org/kskroll.**

Если ваше программное обеспечение не поддерживает автоматическое обновление якорей доверия DNSSEC (RFC 5011) или не настроено для этого должным образом:

Файл ключа для подписания ключей программного обеспечения необходимо обновить вручную. Новый KSK корневой зоны находится здесь: **https://go.icann.org/2DOB7zn**.

Когда происходит обновление KSK?

Обновление KSK — это процесс, а не единичное событие. Приведенные ниже даты являются важнейшими вехами этого процесса, и в это время конечные пользователи могут столкнуться с перебоями в оказании интернет-услуг:

11 октября 2018 года

Предлагаемая дата, когда новый KSK будет впервые использован для подписания.

11 января 2019 года

Предлагаемая дата, когда старый KSK будет объявлен недействительным.

Узнать больше об обновлении ключа, в том числе ознакомиться с ресурсами, содержащими вспомогательную информацию о подготовке к предстоящему изменению, можно здесь: **https://icann.org/kskroll**.

Вы также можете отправить письмо по электронной почте на адрес **globalsupport@icann.org**, указав «Обновление KSK» в строке «Тема», или присоединиться к обсуждению в Twitter, используя хэштег #KeyRoll.

Designed by ICANN Communications | март 2018 года