Безопасность данных переходит на новый этап, где соперником будет квантовый компьютер.

Zoom объявил о внедрении постквантового сквозного шифрования (Сквозное шифрование (End-to-End Encryption, E2EE) – это метод шифрования данных, при котором информация кодируется на уровне отправителя и дешифруется только на уровне получателя. Даже провайдер или сервис, через который проходит сообщение, не имеет доступа к расшифрованным данным.

 Такой подход обеспечивает высокий уровень конфиденциальности, так как только отправитель и получатель могут прочитать сообщение.

 E2EE широко используется в мессенджерах, электронной почте и других приложениях, где важна защита личной информации от несанкционированного доступа." data-html="true" data-original-title="E2EE" >E2EE) в конференции Zoom Meetings. В ближайшем будущем аналогичная защита станет доступной и для Zoom Phone и Zoom Rooms.

В основе постквантового E2EE от Zoom лежит алгоритм Kyber-768, обеспечивающий уровень безопасности, сопоставимый с AES-192. Kyber был выбран институтом NIST в июле 2022 года в качестве криптографического алгоритма, устойчивого к квантовым атакам.

Для включения постквантового E2EE по умолчанию необходимо, чтобы все участники совещания использовали десктопную или мобильную версию Zoom 6.0.10 или выше. Если кто-то из участников не соответствует этому минимальному требованию, будет использоваться стандартное сквозное шифрование.

Хотя квантовые компьютеры все еще находятся на экспериментальной стадии, угроза заключается в том, что квантовые компьютеры смогут легко решать классические математические задачи, считающиеся сложными в вычислениях, что сделает криптоанализ гораздо проще.

Дополнительно стоит учитывать атаку «собери сейчас, расшифруй позже» (Harvest Now, Decrypt Later, «Собери сейчас, расшифруй позже» (Harvest Now, Decrypt Later, HNDL) — это тактика, используемая злоумышленниками, которая заключается в сборе и долгосрочном хранении зашифрованных данных с надеждой на то, что возможность их расшифровать появится в будущем.

 Эта стратегия основана на предположении, что с развитием технологий, в частности квантовых компьютеров, текущие методы шифрования могут стать уязвимыми. Таким образом, даже если злоумышленник не может взломать информацию сегодня, он может ожидать, что сможет это сделать в будущем, когда появятся более мощные инструменты для

дешифровки." data-html="true" data-original-title="HNDL" >HNDL). То есть опытные злоумышленники могут перехватывать и хранить зашифрованный сетевой трафик сейчас, с целью расшифровать его позже, когда квантовые компьютеры станут более мощными.

Постквантовая криптография призвана устранить такие риски, что побудило множество компаний, включая Google , Signal , HP, Amazon Web Services (AWS), Apple, Cloudflare и Tuta, интегрировать новый стандарт в свои продукты.

Несмотря на то, что квантовые компьютеры, способные взломать современную криптографию, пока являются лишь теоретической концепцией, усилия правительств уже направлены на помощь организациям в переходе на устойчивую к квантовым атакам криптографию.