

В России осваивают квантовое шифрование

Российский квантовый центр и компания "КриптоПро" будут сотрудничать в сфере разработки комбинированной системы шифрования, основанной на сочетании классических криптографических методов и квантовой технологии передачи данных.

РКЦ [ведет](#) работы по созданию линий

"абсолютно защищенных от любого прослушивания", причем защита строится не на математической сложности, как это сейчас происходит во всех системах шифрования, а с помощью фундаментальных законов квантового мира, которые говорят о том, что невозможно незаметным образом подсмотреть за одной элементарной частицей. И не потому, что у нас нет хороших приборов или нужны более совершенные приборы, а потому что вступают в силу законы, которые говорят, что вне зависимости от совершенства прибора подсмотреть нельзя, не изменив систему".

Представитель РКЦ Руслан Юнусов отмечает, что такие системы разрабатываются в мире и их можно приобрести у иностранных поставщиков, однако, сотрудники Российского квантового центра локализуют такое решение. Уже разработано устройство для передачи данных через оптоволоконную линию длиной 30 км с защитой посредством квантового ключа шифрования.

"Это один из аспектов, который меняет наш мир, потому что с ростом Интернета вещей и Интернета всего, когда различные объекты будут обмениваться данными или даже будут управляемы через сеть. В этом случае риск взлома будет вести не только к потере денег, но и к опасности для жизни, если такие системы биосовместимы. И поэтому роль безопасности будет возрастать".

Поскольку самостоятельное использование квантово-механических методов шифрования пока далеко от внедрения, РКЦ и компания "КриптоПро" намерены использовать их преимущества в применяемых сейчас массовых криптосредствах. Речь идет о комбинации протоколов классической криптографии и данных, передаваемых по квантовым каналам.

По мнению сотрудника компании "КриптоПро" Станислава Смышляева, такой подход даст возможность изучить перспективы квантового шифрования в реальных условиях, не теряя в качестве, поскольку защита информации будет обеспечиваться хорошо изученными методами. В декабре будущего года [планируется](#) выпустить опытный образец, в котором будет предусмотрена возможность "замешивания" данных, зашифрованных традиционными методами, с передаваемыми по квантовому каналу.