АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕАЛИЗАЦИИ КВАНТОВОГО ШИФРОВАНИЯ

А.С. Кривда

Шифрование информации на протяжении всей своей истории человечество всегда было весьма актуальной темой, поэтому и появилась целая наука – криптография. На сегодняшний день криптография широко используется для защиты данных в сети. Базовой задачей криптографии является шифрование данных и аутентификация отправителя. Это легко выполнить, если отправитель и получатель имеют криптографический ключ. Криптографический ключ – это числовая последовательность определенной длины, созданная для шифрования информации. Перед началом обмена каждый из участников должен получить ключ, причем эту процедуру следует выполнить с наивысшим уровнем конфиденциальности, так, чтобы никакая третья сторона не могла получить доступ даже к части этой информации. Задача безопасной пересылки ключей может быть решена с помощью квантовой криптографии, которая позволяет обеспечить постоянную и автоматическую генерацию ключей. Технология квантового распределения криптографических ключей решает одну из основных задач криптографии – гарантированное распределение ключей между удаленными пользователями по открытым каналам связи, при этом любая попытка злоумышленника вмешаться в процесс передачи криптографических ключей вызовет высокий уровень ошибок. На сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью. Надежность метода основывается на законах квантовой механики.

Необходимо отметить, что проблемы реализации квантового шифрования остаются. Кодировать данные в квантовых состояниях достаточно сложно, для этого нужно уметь генерировать и детектировать одиночный фотон, что является непростой технологической задачей. Так же квантовые состояния уязвимы и могут разрушаться под действием тепловых шумов и других помех. Реальные квантовые устройства остаются уязвимыми для некоторых типов атак [1–3].

Литература

1. Cambridge Journal of science and policy. Quantum Key Distribution: Advantages, Challenges and Policy [Electronic resource]. – Access mode: https://www.repository.cam.ac.uk/bitstream/handle/1810/311529/CJSP_Paper_Lovic.pdf?sequence=1. – Date of access: 28.04.2021.

2. Quantum Cryptography, Explained [Electronic resource]. – Access mode: https://quantumxc.com/quantum-cryptography-explained/. – Date of access: 28.04.2021.

3. Квантовая криптография / шифрование [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/. – Дата доступа: 28.04.2021.