УДК 004.056.5:004.021

Студ. Г.А. Нестеров, В.А. Исаков
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ПРОБЛЕМЫ КВАНТОВОГО ШИФРОВАНИЯ

Криптографические методы – основные средства защиты информации [1]. Квантовая криптография (КК) [2] – это направление в области криптографии, которое использует квантовые свойства для создания защищенных протоколов связи.

В докладе анализируются два протокола КК. Протокол BB84[3], который является одним из примеров асимметричного квантового шифрования и протокол E91, генерация открытого и закрытого ключейиспользует квантовые состояния для создания общего секретного ключа между отправителем и получателем.

КК имеет большой потенциал для защиты информации и защиты конфиденциальности во многих областях (медицинские записи, финансовые транзакции, правительственные данные), однако на данный момент есть ряд проблем, не позволяющих использовать данную технологию массово.

Проблемы заключается в том, что квантовое шифрование требует очень точного, сложного и дорогостоящего оборудования, не является полностью безопасным и не может быть использовано для шифрования больших объемов данных, а для решения этих проблем требуются инвестиции, ресурсы и время.

В результате научной работы проведен сравнительный анализ двух перспективных протоколов квантового шифрования, были выявлены проблемы, а также положительные стороны. На наш взгляд квантовое шифрование имеет потенциал, но на данный момент технология находится в стадии совершенствования.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.

2. Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Черняковский. Квантовая криптография. – МАКС Пресс, 2011. – 111 с.

3. Протокол E91. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/316252/– Дата доступа: 03.04.2023.