Сценарии использования квантовых ключей для передачи квантово-защищенной секретной информации

ЦЫПЫШЕВ В.Н., ФЕДЧЕНКО А.А., ВОРОТНИКОВ В.В., ВИНОГРАДОВ Р.О.

В середине 2020 года на форуме ТК26 был опубликован документ

- Сценарии использования квантовых ключей для передачи квантово-защищенной секретной информации,
- https://tc26.ru/forum/viewtopic.php?f=67&t=1109&sid=63b8517acce1585a32655b56dc0cd5aa

- В указанном документе излагаются различные сценарии применения квантовых ключей в зависимости от места их применения в сети квантовозащищенной связи.

- При этом основными сервисами сети КРК считаются квантовозащищенная магистральная передача данных и квантовозащищенная передача криптографических ключей/секретных значений клиентов сети.

В указанном документе используются следующие термины и обозначения:

- СКЗИ ККС ВРК --- комплект из двух устройств, соединенных высококачественным оптическим и общедоступным каналами связи, и предназначенных для выполнения квантового криптографического протокола. Каждое из устройств называется полукомплектом.
- Сеть КРК --- сеть квантово-защищенного распространения криптографических ключей Клиентов сети, состоящая из модулей доверенных промежуточных узлов и оконечных узлов, располагающих комплектами СКЗИ ККС ВРК, и использующими квантовые ключи для защищенной передачи криптографических ключей и иных секретных значений клиентов, а также для информационного обмена между узлами и модулями сети

- МДПУ --- модуль доверенного промежуточного узла. Состоит из двух и более разнонаправленных полукомплектов СКЗИ ККС ВРК и такого же числа комплектов СКЗИ для высокоскоростного шифрования (магистральное СКЗИ)
- ОУ --- оконечный узел. Состоит из одного или нескольких полукомплектов СКЗИ ККС ВРК и сопряженных магистральных СКЗИ. Основная функция --- хранение и обработка передаваемой по сети КРК информации, а также связь с Клиентом
- Клиент --- потребитель услуг сети КРК. Передает криптографические ключи или секретные значения, используемые для выработки секретных ключей на ОУ через обычные (неквантовые) каналы связи с использованием магистрального СКЗИ. СКЗИ ККС ВРК не имеет.

В документе были рассмотрены следующие вопросы:

- Магистральное шифрование между МДПУ
- Шифрование обмена между различными СКЗИ одного МДПУ
- Маршрутизация при передаче данных внутри МДПУ
- Шифрование обмена между Оконечным узлом и МДПУ
- Шифрование обмена между оконечным узлом и клиентом
- Шифрование обмена между клиентами сети КРК
- Использование предварительно распределенных ключей
- Топология сети КРК. Безопасность и устойчивость сети КРК

- Хотелось бы получить отзывы широкой криптографической общественности на данный документ.