УДК 654.026

«ПРИМЕНЕНИЕ СИСТЕМ КРК В СЕТИ ПЕРЕДАЧИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ»

Негурица А.О. (ВАС), **Грабовой М.Н.** (ИТМО), **Егоров В.И.** (ИТМО)
Научный руководитель – кандидат физико-математических наук, Егоров В.И. (ИТМО)

Введение. В настоящее время можно с уверенностью сказать, что безопасность и разведзащищенность сети передачи данных специального назначения (далее-СПД) обеспечивается в полном объеме. Однако в октябре 2024 года китайские ученые уже заявили об успешной попытке взлома ассиметричного алгоритма RSA с помощью квантового компьютера D-Wave. В ближайшем будущем прогнозируется изобретение квантового компьютера с квантовым объемом, необходимым для взлома симметричных алгоритмов шифрования, в связи с этим безопасность СПД становится под угрозу. В планах компании QuEra Computing в 2026 году представить квантовый компьютер на 10 000 кубитах со 100 логическими кубитами, что уже поставит под угрозу симметричные алгоритмы шифрования.

В целях защиты от квантового компьютера ученые предлагают использовать квантовые коммуникации. Квантовые коммуникации активно развиваются в мире, мировым лидером считается Китай. Страна реализует амбициозные проекты в этой сфере, например, запустила первый в мире квантовый спутник «Мо-цзы» и самую длинную в мире магистральную квантовую линию «Пекин — Шанхай».

В России также есть успехи в области применения квантовых коммуникаций. В конце 2024 года ФСБ сертифицировала новое оборудование для квантовых коммуникаций от компаний «ИнфоТеКС» и «СМАРТС-Кванттелеком». Из этого следует, что данное оборудование можно применять и в СПД.

Основная часть. Для внедрения квантовый коммуникаций в СПД необходимо доказать, что угроза действительно существует. Для этого рассматривается требование к системе связи – разведзащищенность. С помощью математической модели показывается воздействие квантового компьютера на СПД с используемыми ныне средствами защиты. В условиях данной угрозы числовые показатели разведзащищенности оказываются ниже требуемых, что не соответствует заявленным требованиям безопасности СПД. Для повышения безопасности и разведзащищенности СПД предлагается использовать квантовые коммуникации, а именно принцип квантового разделения ключа (далее - КРК). Рассмотрена математическая модель воздействия квантового компьютера на СПД с применением КРК. Показатели времени вскрытия выше требуемых, а значит квантовый компьютер перестанет быть угрозой для СПД.

Выводы. Проведен анализ угроз СПД при использовании противником квантового компьютера. Разработана математическая модель воздействия квантового компьютера на СПД без применения КРК и с применением КРК.

Список использованных источников:

1. https://hightech.fm/2021/08/11/quantum-rails (Дата обращения: 21.01.2025 г.)
2. https://ele74197079.narod.ru/Metod_Sistemi_svyazi_i_opovesheniya_A.S-Belyavskay.pdf (Дата обращения: 24.01.2025 г.)