

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))**

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Квантовые сети и коммуникации

Направление подготовки: 02.03.02 – Фундаментальная информатика и информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Квантовые сети и коммуникации» является формирование у обучающихся комплекса знаний, умений и навыков, необходимых для теоретического анализа и практического построения систем квантовой криптографии.

В курсе изложены необходимые сведения по классической теории информации, а также изучаются основы математического аппарата классической криптографии. В частности, рассматриваются системы симметричного и асимметричного шифрования, одноразовые ключи, критерий Шеннона абсолютной секретности. Изучаются основы аппарата квантовой оптики, необходимые для изучения систем квантовых коммуникаций, в частности, изучаются слабые когерентные и однофотонные состояния. Рассматриваются основные стадии квантовых протоколов распределения ключей. Изучается элементная база систем КРК и виды квантовых каналов связи: способы создания одиночных фотонов (ослабленных когерентных состояний?), детекторы одиночных фотонов, особенности распространения одиночных фотонов по оптоволоконным

каналам связи. Освещаются основные протоколы квантового распределения ключей и изучается их реализация. Рассматриваются методы практической чистки первичных ключей и методы сжатия ключей (усиления секретности) в квантовой криптографии. Рассматриваются различные атаки на системы квантового распределения ключей, в частности, атака с расщеплением по числу фотонов, атака с подменой фазы в системах с фазовым кодированием, атака с ослеплением фотодетекторов. Изучаются методы борьбы с такими атаками. Проводится анализ стойкости квантовых протоколов распределения ключей.

Студенты должны научиться проектировать компьютерные сети с использованием современного сетевого оборудования в соответствии со стандартами и выполнять задачи по настройке оборудования и поддержке работоспособности сети.

Основными задачами дисциплины являются:

- изучить основные принципы и подходы к построению систем квантовой коммуникации и распределенных защищенных сетей на их основе;
- освоить принципы формирования, передачи и регистрации квантовых сигналов в волоконно-оптических и атмосферных каналах передачи данных;
- изучить базовые протоколы, подходы к обоснованию их стойкости, методы экспериментальной реализации;
- овладеть навыками работы с экспериментальными системами квантовой коммуникаций;
- овладеть навыком самостоятельной работы с технической документацией устройств квантовой коммуникации.

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов)).