Задания ДПП «Квантовые технологии и квантовая связь»

Всего заданий: 1

**Задание № 1**

**Тип задания**

Задание на применение умений и навыков в реальных или модельных условиях

**Описание ситуации и постановка задачи**

В соответствии с предлагаемыми ситуациями выбрать верные утверждения

**Место выполнения**

учебный класс/учебный портал

Максимальное время выполнения: 45 минут

**Критерии оценки**

Предмет оценки: «Уметь ориентироваться в методах, принципах и технологиях передачи ключа шифрования с использованием платформы квантового распределения ключей по открытым оптоволоконным линиям»

|  |  |
| --- | --- |
| Объект оценки | Модельный элемент |
| Проанализировать структуру фотонов и квантов, описать как они ведут себя в различных квантовых каналах. Выяснить, какие характеристики сред распространения влияют на передачу квантового сигнала. Выберите верные утверждения: 1. Взаимодействие частиц запутанной пары с окружающей средой приводит к необратимому разрушению исходной запутанности, которая, в свою очередь, приводит к необратимому искажению передаваемого посредством телепортации сигнала 2. Взаимодействие частиц запутанной пары с окружающей средой приводит к укреплению исходной запутанности, которая, в свою очередь, приводит к улучшению достоверности передаваемого посредством телепортации сигнала 3. На передачу квантового сигнала влияет коэффициент хроматической дисперсии 4. На передачу квантового сигнала не влияет коэффициент хроматической дисперсии | 1,3 |
| Проанализировать возможность применения квантовых алгоритмов Шора и ВВ84 для защиты криптографической системы в различных квантовых каналах связи. Выбрать верные утверждения: 1. Протокол ВВ84 будет не эффективен в деполяризующем канале, предпочтительнее применение протокола Шора 2. Протокол Шора будет не эффективен в деполяризующем канале, предпочтительнее применение протокола ВВ84 3. Канал затухания фазы является подобием декогерентизации в реальной физической ситуации, применение протокола Шора и ВВ84 будет такое же, как и для деполяризующего канала 4. В канал затухания фазы не применяются протоколы Шора и ВВ84 | 2,3 |
| Проанализировать защищенность квантового распределения ключей с использованием основных квантовых протоколов и их модификаций. Выбрать верные утверждения: 1. Успешная атака с использованием фальшивых состояний дает Еве полное знание ключа. 2. Успешная атака с использованием фальшивых состояний дает Еве неполное знание ключа. 3. Протокол SARG04 основан на BB84, и не отличается способом детектирования ошибок 4. Протокол SARG04 основан на BB84, но отличается способом детектирования ошибок | 1,4 |
| Проанализировать поведение сигнала в квантовом канале связи на базе основных квантовых уравнений . Выбрать верные утверждения: 1. Можно применить уравнения Шредингера к свободной частице или электрону, который совершает движение вдоль оси ОХ. При этом величина потенциальной энергии частицы, находящейся в свободном движении, равна нулю 2. Можно применить уравнения Шредингера к свободной частице или электрону, который совершает движение вдоль оси ОХ. При этом величина потенциальной энергии частицы, находящейся в свободном движении, равна единицу 3. Волновая функция, характеризующая движение свободной частицы вдоль оси ОХ, будет записана следующим образом: ψ=ψ0e+i(ωt+kx)ψ=ψ0e+i(ωt+kx) 4. Волновая функция, характеризующая движение свободной частицы вдоль оси ОХ, будет записана следующим образом: ψ=ψ0e−i(ωt−kx)ψ=ψ0e−i(ωt−kx) | 1,4 |
| Проанализировать возможности увеличения пропускной способности систем квантовой коммуникации при использовании математической модели квантовых вычислений. Выбрать верные утверждения: 1. Для увеличения пропускной способности можно прибегнуть к созданию системы мультиплексирования для квантовых каналов связи 2. Для увеличения пропускной способности недейственным является наличие неоптимального канала 3. Максимальная пропускная способность определяется размером максимального независимого набора G(X) и низкой вероятностью столкновения, но, возможно, только два независимых входа G(X)|X| 4. Максимальная пропускная способность определяется размером минимального независимого набора G(X) и высокой вероятностью столкновения, но, возможно, только два независимых входа G(X)|X| | 1,3 |