

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Радиофизический факультет

УТВЕРЖДЕНО:

Декан

А. Г. Коротаев

Оценочные материалы по дисциплине

Системы квантовых коммуникаций

по направлению подготовки / специальности

03.04.03 Радиофизика, 12.04.03 Фотоника и оптоинформатика

Направленность (профиль) подготовки/ специализация:

Цифровые технологии фотоники и радиофизики

Форма обучения

Очная

Квалификация

инженер-исследователь

Год приема

2025

СОГЛАСОВАНО:

Руководитель ОП

А.П. Коханенко

Председатель УМК

А.П. Коханенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ПК-1 Способен производить анализ состояния научно-технической проблемы, технического задания, формулировать цель и задачи научного исследования в области профессиональной деятельности.

ПК-2 Способен осуществлять построение математических моделей объектов исследования и выбор готового или разработку нового алгоритма решения.

ПК-3 Способен использовать современное оборудование для решения профессиональных задач.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

РОПК-1.1 Формулирует проблему и определяет предметную область исследования

РОПК-2.1 Формулирует постановку задачи, определяет параметры и функции разрабатываемой системы

РОПК-3.1 Понимает принципы действия устройств и систем, предназначенных для решения профессиональных задач

РОПК-3.2 Проводит измерения с использованием современных устройств и систем для решения профессиональных задач

РОПК-3.3 Обрабатывает и анализирует результаты исследований

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- тесты;
- задачи;
- задания.

Примеры тестовых вопросов (РОПК-1.1, РОПК-2.1, РОПК-3.1, РОПК-3.2, РОПК-3.3):

1. Какой тип кодирования использовали Чарльз Беннет и Жиль Brassar в протоколе квантового распределения ключа BB84?

- а) частотное кодирование
- б) фазовое кодирование
- в) поляризационное кодирование
- г) временное кодирование

2. Потери на единицу длины в квантовом канале составляют 0,05 дБ/км. Приемный и передающий блоки системы квантового распределения ключей расположены на расстоянии 100 км друг от друга. Чему равны общие потери в квантовом канале?

- а) 5 дБ
- б) 100 дБ
- в) 0,5 дБ
- г) 0,05 дБ

3. Во сколько раз просеянный ключ короче сырого ключа в случае протокола квантового распределения ключа BB84?

- а) 3
- б) 0,5
- в) 2
- г) 4

4. Средняя мощность излучения лазера, работающего в импульсном режиме, измеряется в

- а) дБ

- б) Вт
- в) Дж
- г) фотон/импульс

5. Чему равна длина квантового канала, если в результате серии измерений были получены следующие значения: 1,005 км, 0,995 км, 1,003 км, 0,997 км?

- а) 1 км
- б) $(0,997 \pm 0,07)$ км
- в) 0,997 км
- г) $(1 \pm 0,05)$ км

Ключи: 1. в); 2. а); 3. в); 4. б); 5 г).

Критерии оценивания: тест считается пройденным, если обучающийся ответил правильно как минимум на 60 % вопросов.

Примеры задач (РОПК-1.1, РОПК-2.1, РОПК-3.1):

1. Длина накопительной линии в двухпроходной оптоволоконной схеме Plug&Play квантового распределения ключей по протоколу BB84 составляет 25 км. Лазерные импульсы следуют с частотой 5 МГц. Найдите максимальное количество лазерных импульсов в пачке.

2. В двухпроходной оптоволоконной схеме Plug&Play квантового распределения ключей по протоколу BB84 накопительная линия имеет длину 30 км, а квантовый канал – 5 км. Определите за какое время импульс, испущенный лазером, доходит до детектора одиночных фотонов.

3. Система квантового распределения ключей имеет лазер, генерирующий импульсы света с длиной волны 1,55 мкм. Импульсы содержат по 0,1 фотону в среднем, а период их следования составляет 200 нс. Найдите мощность излучаемого лазером света.

4. Лазер, находящийся в передающем блоке системы квантового распределения ключей, работает на длине волны 810 нм и излучает импульсы света с частотой следования 50 МГц. Средняя мощность лазерного излучения составляет 10 мкВт. Какого номинала аттенуатор необходимо установить на выходе передающего блока, чтобы выходящие из него лазерные импульсы содержали в среднем по 0,1 фотону?

5. Чтобы шифровать на лету голос человека методом одноразовых блокнотов, нужен ключ, генерируемый со скоростью 5 кбит/с. Пусть лазерные импульсы, следующие с частотой 1 ГГц, содержат в среднем 0,1 фотон на импульс; потери в квантовом канале составляют 0,3 дБ/км; детектор способен зарегистрировать 10 % приходящих на него лазерных импульсов. Найдите максимальное расстояние квантового распределения ключа по протоколу BB84 для шифрования голоса.

Ответы: 1. 1250 импульсов; 2. 350 мкс; 3. 500 мкс; 4. 0,1 %; 5. $6,4 \cdot 10^{-14}$ Вт; 6. 69,1 дБ; 7. 110 км; 8. 525 кбит/с

Критерии оценивания:

Результат решения задачи оценивается баллами в диапазоне от 0 до 3 включительно.

3 балла выставляются если, задача решена без ошибок и обучающийся способен объяснить решение задачи.

2 балла выставляется, если задача решена без ошибок, но при этом обучающийся испытывает затруднения в объяснении решения задачи.

1 балл выставляется, если задача решена без ошибок, но при этом обучающийся испытывает сильные затруднения в объяснении решения задачи.

0 баллов выставляется, если задача не решена, либо решена с ошибками, либо обучающийся не может объяснить решение задачи.

Примеры заданий (РОПК-1.1, РОПК-3.1, РОПК-3.2, РОПК-3.3):

1. Измерить величину потерь в передающем блоке двухпроходной оптоволоконной системы Plug&Play квантового распределения ключей по протоколу BB84.
2. Провести измерение длины оптоволоконного квантового канала, а также потерь на километр и общих потерь в нем. Выявить наличие дефектов, определить их тип и местоположение.
3. Определить величину темнового счета детектора одиночных фотонов.
4. Измерить зависимость квантовой эффективности детектора одиночных фотонов от среднего количества фотонов в лазерном импульсе.
5. Определить время прихода первого лазерного импульса пачки импульсов на детектор одиночных фотонов в двухпроходной оптоволоконной системы Plug&Play квантового распределения ключей по протоколу BB84. Сравнить полученное значение с теоретическим.

Критерии оценивания:

Результат выполнения задания оценивается баллами в диапазоне от 0 до 3 включительно.

3 балла выставляются, если обучающийся выбрал верную методику измерения параметров и способен ее объяснить; демонстрирует умение пользоваться приборами и устройствами для проведения измерений; получил верные значения измеряемых параметров; произвел правильную обработку результатов измерения; способен провести анализ результатов измерений.

2 балла выставляется, если обучающийся выбрал верную методику измерения параметров, но испытывает затруднения при ее объяснении; демонстрирует умение пользоваться приборами и устройствами для проведения измерений; получил верные значения измеряемых параметров; произвел обработку результатов измерения с небольшими отклонениями; испытывает затруднения при анализе результатов измерения.

1 балл выставляется, если обучающийся: выбрал верную методику измерения параметров, но испытывает сильные затруднения при ее объяснении; демонстрирует фрагментарное умение пользоваться приборами и устройствами для проведения измерений; получил значения измеряемых параметров с отклонением от верных; произвел обработку результатов измерений с ошибками; испытывает сильные затруднения при анализе результатов измерений.

0 баллов выставляется, если, обучающийся: выбрал неверную методику измерения параметров, либо методика выбрана верно, но не способен ее объяснить; не умеет либо демонстрирует фрагментарное умение пользоваться приборами и устройствами для проведения измерений; получил неверные значения измеряемых параметров; произвел неверно обработку результатов измерений; не способен провести анализ результатов измерений.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

К итоговому контролю допускаются обучающиеся выполнившие все тесты, задачи и задания текущего контроля. На зачет выносится решение двух кейсов.

Первый кейс проверяет сформированность у обучающегося РОПК-1.1, РОПК-2.1, РОПК-3.1, РОПК-3.3. Ответ дается в устной форме.

Второй кейс проверяет сформированность у обучающегося РОПК-1.1, РОПК-3.1, РОПК-3.2, РОПК-3.3. Ответ дается в устной форме.

Пример первого кейса:

«Разработка технического задания на систему квантового распределения ключей для внедрения в корпоративную сеть»

1. Описание ситуации:

Компания «ГарантСвязь» является провайдером высокозащищенных телекоммуникационных услуг для крупных финансовых организаций и правительственных структур. В связи с растущими угрозами кибербезопасности и потенциальной уязвимостью классических методов шифрования, руководство компании рассматривает внедрение системы квантового распределения ключей (КРК) для усиления защиты своих каналов связи между двумя дата-центрами, расположенными в черте города.

2. Цель:

Разработать техническое задание на систему КРК, которое будет служить руководством для команды инженеров при реализации проекта.

3. Ожидаемые результаты:

- Определение функциональных и иных требований к системе КРК.
- Выбор подходящего под решаемую задачу протокола КРК.
- Выбор архитектуры системы КРК и ее компонентов.
- Формулировка потенциальных рисков и ограничений при внедрении системы КРК.

Пример второго кейса:

«Тихий сбой в квантовой сети»

1. Описание ситуации:

Компания «ИмпульсТелеком» эксплуатирует квантовую сеть на основе двухпроходной оптоволоконной системы Plug&Play квантового распределения ключей (КРК) по протоколу BB84, соединяющую два критически важных дата-центра. Связь осуществляется по выделенной оптоволоконной линии протяженностью порядка 10 км. Система КРК перестала распределять ключи. Канал связи, используемый для согласования ключей, работает без сбоев. Система КРК используется для защиты критически важных данных. Сбой ставит под угрозу конфиденциальность и безопасность обмена информацией.

2. Цель:

Выявить и устранить причину неисправности как можно быстрее.

3. Первоначальные условия:

В вашем распоряжении имеется:

- детектор повреждения оптического волокна,
- микроскоп для оптических разъемов,
- источник оптического излучения,
- измеритель оптической мощности,
- оптический рефлектометр,
- сварочный аппарат,
- скалыватель оптического волокна,
- стриппер для оптического волокна,
- расходные материалы для сварки оптического волокна и чистки оптических разъемов,
- оптоволоконные компоненты,
- специализированное ПО системы КРК,
- документация системы КРК.

4. Ожидаемые результаты:

- Выдвижение гипотез о возможных неисправностях в системе КРК.
- Формулировка плана действий по выявлению неисправности в системе КРК.
- Выявление первопричины отсутствия распределения ключей.
- Устранение неисправности.
- Настройка системы КРК для возвращения к нормальной работе.
- Формулировка рекомендаций для предотвращения подобных сбоев в будущем.

Критерии оценивания:

Результат решения первого кейса оценивается баллами в диапазоне от 0 до 10 включительно.

8-10 баллов выставляются, если обучающийся демонстрирует понимание технологии КРК и ее особенностей; полно и четко определил требования к внедряемой системе КРК; логично и обоснованно выбрал протокол и архитектуру системы КРК; сформулировал потенциальные риски и ограничения при внедрении системы КРК; структурированно и ясно изложил техническое задание.

5-7 баллов выставляется, если обучающийся демонстрирует понимание технологии КРК и ее особенностей; не в полной мере определил требования к внедряемой системе КРК; необоснованно выбрал протокол и архитектуру системы КРК; испытывает затруднения в формулировке потенциальных рисков и ограничений при внедрении системы КРК; не в полной мере структурированно и ясно изложил техническое задание.

2-4 баллов выставляется, если обучающийся демонстрирует фрагментарное понимание технологии КРК и ее особенностей; испытывает затруднения в определении требований к внедряемой системе КРК; испытывает затруднения с выбором протокола и архитектуры системы КРК; не может сформулировать или испытывает сильные затруднения в формулировке потенциальных рисков и ограничений при внедрении системы КРК; не структурированно и неясно изложил техническое задание.

0-1 баллов выставляется, если обучающийся не понимает технологию КРК и ее особенности; не определил или испытывает сильные затруднения в определении требований к внедряемой системе КРК; не может выбрать или испытывает сильные затруднения с выбором протокола и архитектуры системы КРК; не может сформулировать или испытывает сильные затруднения в формулировке потенциальных рисков и ограничений при внедрении системы КРК; не структурированно и неясно изложил техническое задание.

Результат решения второго кейса оценивается баллами в диапазоне от 0 до 10 включительно.

8-10 баллов выставляются, если обучающийся выдвинул всевозможные гипотезы о возможных неисправностях в системе КРК; сформулировал логически верный план действий по выявлению неисправности в системе КРК; выявил правильно первопричину сбоя в работе системы КРК; устранил неисправность; настроил систему КРК для возвращения к нормальной работе; сформулировал рекомендации для предотвращения подобных сбоев в будущем.

5-7 баллов выставляется, если обучающийся выдвинул основные гипотезы о возможных неисправностях в системе КРК; сформулировал план по выявлению неисправности в системе КРК, последовательность действий в котором логически нарушена, но который позволяет выявить первопричину сбоя в работе системы КРК; выявил правильно первопричину сбоя в работе системы КРК; устранил неисправность; настроил систему КРК для возвращения к нормальной работе, либо определил все настроечные параметры, но не добился снижения QBER до уровня 5 % и меньше; испытывает затруднения с формулировкой рекомендаций для предотвращения подобных сбоев в будущем.

2-4 баллов выставляется, если обучающийся испытывает затруднения в выдвижении гипотезы о возможных неисправностях в системе КРК; испытывает затруднения в формулировке плана по выявлению неисправности в системе КРК; последовательность действий в предложенном плане логически нарушена; выявил правильно первопричину сбоя в работе системы КРК; устранил, либо не устранил неисправность; не смог настроить систему КРК для возвращения к нормальной работе, определил не все настроечные параметры; не сформулировал, либо испытывает затруднения с формулировкой рекомендаций для предотвращения подобных сбоев в будущем.

0-1 баллов выставляется, если обучающийся не смог выдвинуть ни одной гипотезы о возможных неисправностях в системе КРК, либо выдвинул гипотезы, среди которых нет правильной; не сформулировал, либо сформулировал не верный план действий по выявлению неисправности в системе КРК; не выявил правильно первопричину сбоя в работе системы КРК; не устранил неисправность; не настроил систему КРК для возвращения к нормальной работе; не сформулировал рекомендации для предотвращения подобных сбоев в будущем.

Итоговая оценка по дисциплине формируется путем суммирования баллов за текущий контроль (максимум 80 баллов) и итоговый контроль (максимум 20 баллов) с последующим переходом к пятибалльной шкале:

- Оценка «отлично» выставляется, если набрано 90-100 баллов.
- Оценка «хорошо» выставляется, если набрано 75-89 баллов.
- Оценка «удовлетворительно» выставляется, если набрано 60-74 балла.
- Оценка «неудовлетворительно» выставляется, если набрано менее 60 баллов.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примеры тестовых вопросов:

1. Какой тип кодирования используют в спутниковом квантовом канале связи, использующем спутник «Мо-цзы»? (РОПК-1.1, РОПК-3.1)
 - а) фазовое кодирование
 - б) поляризационное кодирование
 - в) частотное кодирование
 - г) временное кодирование
2. Среднее количество фотонов, содержащихся в лазерном импульсе, составляет 0,1 фотон/импульс. Какова вероятность, что в лазерном импульсе будет содержать один фотон? (РОПК-1.1, РОПК-2.1)
 - а) 0,1
 - б) 0,8
 - в) 1
 - г) 0,9
3. Как соотносятся между собой длины сырого и просеянного ключа в протоколе с шестью квантовыми состояниями? (РОПК-1.1, РОПК-2.1, РОПК-3.1)
 - а) Длина сырого ключа в 3 раза больше, чем длина просеянного ключа
 - б) Длина сырого ключа в 3 раза меньше, чем длина просеянного ключа
 - в) Длина сырого ключа в 2 раза больше, чем длина просеянного ключа
 - г) Длина сырого ключа в 2 раза меньше, чем длина просеянного ключа
4. Потери в квантовом канале измеряются в (РОПК-1.1, РОПК-3.2)
 - а) Дж
 - б) Вт
 - в) дБ
 - г) фотон/импульс

5. Чему равна средняя мощность лазера, если в результате серии измерений были получены следующие значения: 7,1 мкВт, 6,95 мкВт, 6,97мкВт, 7,01 мкВт, 6,97 мкВт? (РОПК-1.1, РОПК-3.3)

- а) $(7 \pm 0,1)$ мкВт
- б) $(6,97 \pm 0,05)$ мкВт
- в) 7 мкВт
- г) 6,97 мкВт

Ключи: 1. б); 2. г); 3. а); 4. в); 5 а).

Информация о разработчиках

Каширский Данила Евгеньевич, кандидат физико-математических наук, кафедра квантовой электроники и фотоники, доцент