ГОУ ВПО Российско-Армянский (Славянский) университет

Утверждено
Директор Института _____
А.К. Агаронян

«30» апреля 2025г., протокол № 05

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

Наименование дисциплины: Б1.В.06 Квантовая криптография

Автор (ы) к.ф.-м.н., старший преподаватель Газазян Эмиль Альфредович
Ф.И.О, ученое звание (при наличии), ученая степень (при наличии)

Направление подготовки: 11.03.04 Электроника и наноэлектроника
Наименование образовательной программы: Квантовая информатика

Согласовано:

Заведующий Кафедрой общей физики и квантовых наноструктур

Айрапетян Д.Б.

(подпись)

1. **АННОТАЦИЯ**

1.1. Краткое описание содержания данной дисциплины;

Квантовая криптография — это область науки, находящаяся на пересечении квантовой физики и криптографии, в которой используются квантовые свойства частиц (например, суперпозиция и запутанность) для обеспечения абсолютно безопасной передачи информации.

1.2. Трудоемкость в академических кредитах и часах, формы итогового контроля (экзамен/зачет);

Объём дисциплины: 5 зачетных единиц, 180 академических часов

В том числе:

Лекции – 16 часов

Практические занятия – 16 часов

Контрольные мероприятия – 54 часа

Самостоятельная работа – 94 часа

1.3. Взаимосвязь дисциплины с другими дисциплинами учебного плана специальности (направления)

Квантовое программирование, Программирование в физике, Структуры данных и алгоритмы, Функциональное программирование.

1.4. Результаты освоения программы дисциплины:

Код компетенции *(в соответствии рабочим с учебным планом)*	**Наименование компетенции** *(в соответствии рабочим с учебным планом)*	**Код индикатора достижения компетенций** *(в соответствии рабочим с учебным планом)*	**Наименование индикатора достижений компетенций***(в соответствии рабочим с учебным планом)*
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные	УК-2.1	Знает виды ресурсов и ограничений для решения профессиональных задач и основные методы оценки

	способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2 УК-2.3	разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения и анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности Владеет методиками разработки цели и задач проекта, методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией
ПК-2	Способен разрабатывать эффективные алгоритмы решения сформулированных задач с использованием современных языков программирования и обеспечивать их программную реализацию	ПК-2.1 ПК-2.2 ПК-2.3	Знает методы разработки эффективных алгоритмов решения научно-исследовательских задач Умеет использовать алгоритмы решения исследовательских задач с использованием современных языков программирования Владеет навыками разработки стратегии и методологии исследования изделий микро- и наноэлектроники

2. **УЧЕБНАЯ ПРОГРАММА**

2.1. Цели и задачи дисциплины

Цель дисциплины – формирование у студентов фундаментальных знаний и практических навыков в области квантовой криптографии как современного направления информационной безопасности, основанного на физических принципах квантовой механики.

Дисциплина направлена на изучение теоретических основ, квантовых протоколов распределения ключей, физических реализаций квантовых криптосистем, а также анализа их устойчивости к возможным атакам.

Задачи дисциплины:

- **Сформировать** у студентов представление о физических принципах, лежащих в основе квантовой криптографии
- **Ознакомить** с базовыми квантовыми протоколами распределения ключей
- **Показать** роль квантовых эффектов (суперпозиции, запутанности, неопределенности) в обеспечении информационной безопасности
- **Научить** применять методы постобработки (коррекции ошибок, информационной перегонки)
- **Обосновать** необходимость перехода к квантовым и постквантовым методам защиты в условиях развития квантовых вычислений

2.2. Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах) ***(удалить строки, которые не будут применены в рамках дисциплины)***

Виды учебной работы	**Всего, в акад. часах**	**Распределение по семестрам**
		8 сем.
1	**2**	**8**
1. **Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:**	**180**	**180**
1.1. Аудиторные занятия, в т. ч.:	**32**	**32**
1.1.1. Лекции	**16**	**16**
1.1.2. Практические занятия, в т. ч.	**16**	**16**
1.2. Самостоятельная работа, в т. ч.:	**94**	**94**
1.2.1. Подготовка к экзаменам		
1.2.1.1. Курсовые работы		
1.3. Консультации		

1.4. Другие методы и формы занятий		
Итоговый контроль (Экзамен, Зачет, диф. зачет - указать)	Экзамен 54	Экзамен 54

2.3. Содержание дисциплины

2.3.1. **Тематический план и трудоемкость аудиторных занятий (модули, разделы дисциплины и виды занятий) по рабочему учебному плану**

Разделы и темы дисциплины	**Всего (ак. часов)**	**Лекции(ак. часов)**	**Практ. Занятия (ак. часов)**
1	**2=3+4+5+6+7**	**3**	**4**
Тема .1. Основы квантовой теории и принципы криптографии	**6**	**3**	**3**
Тема .2Протоколы квантового распределения ключей (QKD)	**5**	**3**	**2**
Тема 3. Безопасность, атаки и уязвимости квантовых систем	**7**	**4**	**3**
Тема 4. Безопасность, атаки и уязвимости квантовых систем	**4**	**2**	**2**
Тема 5. Архитектура и элементы квантовых сетей	**3**	**1**	**2**
Тема 6. Квантовая криптография в ИБ и правовом контексте	**3**	**1**	**2**
Тема 7. Моделирование и экспериментальные задачи	**4**	**2**	**2**
ИТОГО	**32**	**16**	**16**

2.3.2. **Краткое содержание разделов дисциплины в виде тематического плана**

Тема 1. Основы квантовой теории и принципы криптографии [1,2]

Рассматриваются базовые положения квантовой механики, необходимые для понимания квантовой криптографии: принцип суперпозиции, запутанность, измерения и неопределенность. Проводится обзор классической криптографии и обоснование необходимости квантовых методов защиты информации.

Тема 2. Протоколы квантового распределения ключей (QKD)[1,2]

Изучаются основные протоколы квантового распределения ключей, а также их модификации и практические реализации. Анализируется процесс генерации и обмена ключами через квантовые каналы с последующей классической обработкой.

Тема 3. Безопасность, атаки и уязвимости квантовых систем [1,2]

Анализируются возможные атаки на квантовые криптографические системы, включая перехват и повторную передачу, атаки с использованием квантовой памяти и лазерных импульсов. Рассматриваются методы обнаружения атак и способы обеспечения информационной безопасности в квантовых протоколах.

Тема 4. Физические реализации: фотонные и оптические системы [1,2]

Описываются реальные физические устройства и технологии, используемые в квантовой криптографии: одиночные фотонные источники, модуляторы, интерферометры, детекторы и волоконно-оптические каналы. Обсуждаются технические ограничения и ошибки измерений.

Тема 5. Архитектура и элементы квантовых сетей [1,2]

Рассматриваются принципы построения квантовых сетей и многоузловых систем связи, включая квантовые ретрансляторы, спутниковую связь и перспективы построения глобального квантового интернета. Обсуждается взаимодействие квантовых и классических каналов.

Тема 6. Квантовая криптография в информационной безопасности и правовом контексте [1,2]

Анализируется роль квантовой криптографии в современных системах защиты информации. Рассматриваются международные стандарты, правовые аспекты использования квантовой криптографии, а также перспективы внедрения в критическую инфраструктуру.

Тема 7. Моделирование и экспериментальные задачи [1,2]

Проводится моделирование работы квантовых криптографических протоколов на программном уровне. Выполняются лабораторные эксперименты с симуляторами квантовой связи и анализируются параметры устойчивости и эффективности различных реализаций.

2.3.3. **Краткое содержание практических занятий**

1. Принципы квантовой механики в криптографии

Обсуждение роли квантовой неопределенности, суперпозиции и запутанности в обеспечении безопасности передачи данных. Разбор фундаментальных отличий между классической и квантовой криптографией.

2. Анализ протокола BB84 и его реализаций

Коллективный анализ работы протокола BB84. Обсуждение различных вариантов реализации: с поляризацией фотонов, фазовыми сдвигами и временными метками.

3. Уязвимости и атаки на квантовые каналы

Рассмотрение возможных стратегий атаки на протоколы квантовой криптографии (например, intercept-resend, Trojan-horse, photon number splitting). Обсуждение методов обнаружения атак и стратегий защиты.

4. Практические ограничения физических реализаций

Обсуждение реальных проблем, возникающих при реализации квантовой криптографии: потери в канале, фоновый шум, ошибки регистрации, несовершенства источников фотонов и детекторов.

5. Архитектура квантовых сетей и распределённых систем

Коллективное обсуждение задач построения квантовых сетей, роли ретрансляторов и узлов, а также перспектив спутниковой квантовой связи.

6. Квантовая криптография в системах информационной безопасности

Обсуждение интеграции квантовой криптографии в существующие ИБ-системы и инфраструктуры. Анализ правовых и этических аспектов использования квантовой защиты.

7. Сравнительный анализ классических и квантовых криптосистем

Групповой анализ преимуществ и недостатков квантовой криптографии по сравнению с RSA, ECC и пост квантовыми алгоритмами.

8. Моделирование и интерпретация результатов симуляций

Рассмотрение результатов лабораторных и программных симуляций. Обсуждение типовых ошибок моделирования и методов их устранения. Интерпретация данных с точки зрения теории информации и безопасности.

2.3.4. **Материально-техническое обеспечение дисциплины**

1. Учебные помещения и оборудование:

- Аудитории, оборудованные мультимедийным проектором и доской;

- Компьютерный класс с выходом в интернет (не менее 1 ПК на 2 студентов);

2. Программное обеспечение:

- Пакеты моделирования квантовых систем:
- Quantum Toolbox in Python (QuTiP)
- IBM Quantum Lab (Qiskit)
- SimulaQron, QKDsim или другие симуляторы квантовых сетей

Среда программирования:

- Python 3.x, JupyterLab/Notebook

2.4. Модульная структура дисциплины с распределением весов по формам контролей

Формы контролей	**Вес формы (форм) текущего контроля в результирующей оценке текущего контроля (по модулям)**		**Вес формы промежуточного контроля в итоговой оценке промежуточного контроля**		**Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей**		**Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей (семестровой оценке)**	**Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля**
Вид учебной работы/контроля	**M1[1]**	**M2**	**M1**	**M2**	**M1**	**M2**		
Контрольная работа *(при наличии)*			0.5	0.5				
Устный опрос *(при наличии)*								
Тест *(при наличии)*								
Лабораторные работы *(при наличии)*	0.5	0.5						
Письменные домашние задания *(при наличии)*								
Реферат *(при наличии)*								
Эссе *(при наличии)*								
Проект *(при наличии)*								
Решение задач	0.5	0.5						
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей					0.5	0.5		
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей								

[1] Учебный Модуль

Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей							0.5	
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей							0.5	
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля								0.5
Вес итогового контроля (Экзамен/зачет) в результирующей оценке итогового контроля								0.5
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

3. **Теоретический блок** ***(указываются материалы, необходимые для освоения учебной программы дисциплины)***

3.1. Материалы по теоретической части курса

3.1.1. Учебник(и);

1. M.A. Nielsen, I.L. Chuang — Quantum Computation and Quantum Information. — Cambridge University Press, 10th Anniversary Edition, 2010.
   (Глава 12 посвящена квантовой криптографии; фундаментальный источник по всей области.)
2. Bennett C.H., Brassard G. — Quantum cryptography: Public key distribution and coin tossing.
   Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984.

4. **Фонды оценочных средств** ***(указываются материалы, необходимые для проверки уровня знаний в соответствии с содержанием учебной программы дисциплины).***

4.1. Планы практических занятий

Практическое занятие 1 — Основы квантовой механики для криптографии

Темы: суперпозиция, измерение, запутанность. Работа с симуляторами.

Практическое занятие 2 — Протокол BB84: алгоритм и моделирование

Темы: создание квантовых битов, выбор базисов, обмен ключами. Пример на Python/Qiskit.

Практическое занятие 3 — Анализ атак: intercept-resend и photon number splitting
Темы: имитация атак, восстановление ключа, обнаружение вмешательства.

Практическое занятие 4 — Реализация квантовой связи в волоконно-оптическом канале
Темы: потери, шум, синхронизация. Работа с моделью в QuTiP.

Практическое занятие 5 — Постобработка: информационная перегонка и исправление ошибок
Темы: алгоритмы Cascade, LDPC-коды.

Практическое занятие 6 — Моделирование квантовой сети передачи ключей
Темы: многоузловая топология, квантовые ретрансляторы, гибридные сети.

Практическое занятие 7 — Сравнение квантовой и постквантовой криптографии
Темы: обзор алгоритмов, оценка времени шифрования и стойкости к взлому.

Практическое занятие 8 — Контрольная практика: защита проекта или моделирование протокола
Темы: индивидуальные или групповые задания по моделированию, защита решений.

4.2. Материалы по практической части курса

4.2.1. Учебно-методические пособия;

1.M.A. Nielsen, I.L. Chuang — Quantum Computation and Quantum Information. — Cambridge University Press, 10th Anniversary Edition, 2010.
(Глава 12 посвящена квантовой криптографии; фундаментальный источник по всей области.)

2.Bennett C.H., Brassard G. — Quantum cryptography: Public key distribution and coin tossing .Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984.

4.3. Вопросы и задания для самостоятельной работы студентов

1. В чем заключается отличие классических и квантовых битов?
2. Объясните принцип действия квантового распределения ключей (QKD) в протоколе BB84.
3. Что такое квантовая запутанность и как она используется в криптографии?
4. Какие типы атак возможны в квантовых криптографических системах?
5. Обоснуйте, почему невозможно клонировать произвольное квантовое состояние.
6. В чем состоит принцип «обнаружения вмешательства» в квантовых протоколах?
7. Перечислите и охарактеризуйте физические устройства, используемые в системах QKD.
8. Как обеспечивается коррекция ошибок и конфиденциальность после передачи ключа?
9. В чем заключается роль классического канала в квантовой криптографии?
10. Какие современные проекты и компании занимаются коммерческими QKD-системами?

4.4. Тематика курсовых работ и других форм самостоятельных работ

- История и развитие квантовой криптографии: от BB84 до коммерческих систем
- Протокол BB84: принципы, реализация, уязвимости
- Квантовая запутанность как ресурс в криптографии
- Физические реализации QKD-систем: источники, каналы и детекторы
- Роль теоремы о невозможности клонирования в квантовой безопасности
- Протоколы B92, E91 и SARG04: сравнительный анализ
- Перехват и защита: типы атак на квантовые каналы
- Квантовые ретрансляторы и возможность создания квантового интернета
- Практические проблемы реализации квантовой криптографии в городских сетях
- Применение алгоритмов коррекции ошибок в QKD
- Квантовая криптография в спутниковых каналах связи
- Этика и право в использовании квантовой криптографии
- Постквантовая криптография и её отличие от квантовой
- Сравнение эффективности RSA, ECC и QKD в условиях угроз квантовых атак
- Архитектура гибридных (квантово-классических) систем информационной безопасности

- Перспективы внедрения квантовой криптографии в критическую инфраструктуру
- Квантовые генераторы случайных чисел и их применение в ИБ
- Международные стандарты и сертификация квантовых криптографических решений
- Моделирование квантового канала с шумом и потерями
- Прогноз развития глобальных квантовых сетей и риски кибербезопасности будущего

4.5. Образцы вариантов контрольных работ, тестов и/или других форм текущих и промежуточных контролей

Часть I. Термины и определения (ответ в 1–2 предложениях)

Что такое кубит?

Объясните принцип неопределенности Гейзенберга.

Что означает «квантовая запутанность»?

Назовите ключевое отличие между классическим битом и кубитом.

Что такое квантовая атака типа «intercept-resend»?

Часть II. Вопросы с развернутым ответом

Опишите протокол BB84. В чем его идея и как обеспечивается безопасность?

Приведите возможные ошибки, возникающие в канале квантовой связи, и способы их устранения.

Сравните принципы работы BB84 и B92.

Объясните невозможность клонирования произвольного квантового состояния и её значение для криптографии.

Как обеспечивается выявление перехвата в квантовом протоколе?

Часть III

Какой физический элемент используется для создания одиночных фотонов?

а) Оптический фильтр

б) Лазер с пониженными импульсами

в) Дифракционная решетка

г) Детектор APD

Какое утверждение верно?

а) Квантовая криптография заменяет хэш-функции

б) Квантовые ключи могут быть использованы совместно с классическими алгоритмами

в) BB84 не защищен от прослушивания

г) RSA устойчив к квантовым атакам

4.6. Перечень экзаменационных вопросов

1. Основные принципы квантовой механики, лежащие в основе квантовой криптографии
2. Квантовый бит (кубит): определение, свойства и отличие от классического бита
3. Принцип суперпозиции и его роль в квантовой передаче информации
4. Квантовая запутанность и её применение в криптографических протоколах
5. Протокол BB84: структура, базисы, принципы безопасности
6. Проблема невозможности клонирования квантового состояния и её криптографическое значение
7. Протоколы согласования ключей в условиях шумного канала
8. Типы атак на квантовые криптографические системы (intercept-resend, Trojan-horse и др.)
9. Методы обнаружения перехвата и проверки безопасности в протоколах QKD
10. Физические компоненты квантовой криптосистемы: источники фотонов, поляризаторы, детекторы
11. Особенности передачи квантовых состояний через волоконно-оптические каналы
12. Моделирование квантового канала: влияние потерь и шумов
13. Алгоритмы постобработки: коррекция ошибок и информационная перегонка
14. Аппаратная реализация квантовой криптографии и её ограничения
15. Принципы построения квантовых коммуникационных сетей
16. Квантовые ретрансляторы и перспективы построения квантового интернета
17. Сравнение квантовой и постквантовой криптографии

18. Применение квантовой криптографии в информационной безопасности и защите критической инфраструктуры
19. Международные стандарты и правовое регулирование в области квантовой криптографии
20. Обзор современных коммерческих решений в области QKD
21. Перспективы развития квантовых сетей в глобальном масштабе

4.7. Образцы экзаменационных билетов

Билет №1

1.Принцип суперпозиции и его роль в квантовой криптографии
2.Структура и этапы протокола BB84
3.Смоделируйте передачу 4 кубитов в протоколе BB84 и определите результат в случае совпадения и несовпадения базисов у Алисы и Боба

Билет №2

1.Квантовая запутанность: определение и криптографическое применение
2.Особенности протокола E91 и проверка неравенства Белла
3.Рассчитайте вероятность ошибок в QKD-канале с 10% потерь и 5% шумом

Билет №3

1.Теорема о невозможности клонирования и её значение для безопасности
2.Типы атак на квантовые протоколы: intercept-resend, photon-number splitting
3.Смоделируйте атаку «intercept-resend» на протокол BB84 и проанализируйте, как её можно обнаружить

4.8. Образцы экзаменационных практических заданий

Задание 1. Моделирование протокола BB84
Смоделируйте работу квантового протокола BB84 на наборе из 8 бит.

Сформируйте случайную бинарную строку (сообщение Алисы).

Примените случайные базисы (Z и X) для кодирования.

Смоделируйте выбор базисов Бобом и определите полученные биты.

Найдите позиции совпадения базисов и извлеките ключ.

Введите в модель перехватчика (атака intercept-resend) и вычислите долю ошибок.

Задание 2. Анализ уязвимости квантового канала
Вам даны данные квантового протокола, в котором Алиса передала 10 бит, из них 4 были перехвачены и повторно отправлены.

Проанализируйте, на каких позициях возможны ошибки.

Рассчитайте вероятность обнаружения атаки.

Оцените количество информации, которое потенциально узнал злоумышленник.

Предложите меры по усилению безопасности на этапе постобработки.

Задание 3. Физическая реализация квантового канала
На основе представленных характеристик оборудования:

Длина волны: 1550 нм

Потери на 1 км: 0.2 дБ

Расстояние: 20 км

Эффективность детектора: 0.3

Выполните:

Рассчитайте общие потери в линии связи.

Оцените вероятность регистрации сигнала.

Определите, насколько надёжна передача ключей при таком расстоянии.

Предложите способы повышения эффективности системы.

5. **Методический блок**
   5.1. Методика преподавания
      5.1.1. Методические рекомендации для студентов по подготовке к семинарским, практическим или лабораторным занятиям, по организации самостоятельной работы студентов при изучении конкретной дисциплины.

Подготовка к практическим занятиям

- Заранее изучайте тему: перед каждым семинаром рекомендуется прочитать соответствующую главу из учебника или рекомендованной статьи (список дается преподавателем).

- Выписывайте ключевые понятия: подготовьте определения терминов (кубит, суперпозиция, протокол BB84, запутанность и др.).
- Анализируйте примеры: разберите заранее примеры из лекций и практики, чтобы уверенно участвовать в обсуждении.
- Формулируйте аргументы: если предусмотрены дискуссии (например, сравнение BB84 и RSA), подготовьте позицию, примеры и вопросы к оппонентам.
- Используйте научные источники: старайтесь опираться на статьи из IEEE, arXiv, Springer и др. для расширения понимания и обоснования своей точки зрения.