

Аннотация

Дисциплина «Математические модели квантовых вычислений» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности/специализации «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина не является обязательной при освоении обучающимся образовательной программы и направлена на углубленное формирование следующих компетенций:

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований»

Содержание дисциплины охватывает круг вопросов, связанных с изучением, анализом, разработкой моделей квантовых вычислительных процедур, оценкой угроз для классической криптографии, а также применением законов квантовой механики для обеспечения безопасности данных.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (5 семестр), дифференцированного зачета (6 семестр).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины – формирование у студентов теоретической базы и практических навыков для разработки квантовых моделей и применения квантовых технологий для защиты данных.

1.2. Дисциплина является факультативной дисциплиной по направлению образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований	ПК-3.3.1 знает методы и средства планирования и организации исследований и разработок ПК-3.У.1 умеет применять актуальную нормативную документацию в соответствующей области знаний ПК-3.В.1 владеет навыками организации сбора и изучения научно-технической информации по теме исследований и разработок

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Информатика»,
- «Основы программирования»,
- Базовое представление о протоколах квантового распределения ключей

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- « Основы квантовых алгоритмов в защите информации»

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам	
		№5	№6
1	2	3	4
Общая трудоемкость дисциплины,	4/ 144	2/ 72	2/ 72

ЗЕ/ (час)			
Из них часов практической подготовки	34	17	17
Аудиторные занятия , всего час.	68	34	34
в том числе:			
лекции (Л), (час)	34	17	17
практические/семинарские занятия (ПЗ), (час)	34	17	17
лабораторные работы (ЛР), (час)			
курсовой проект (работа) (КП, КР), (час)			
экзамен, (час)			
Самостоятельная работа , всего (час)	76	38	38
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет, Дифф. зач.,	Зачет,	Дифф. зач.,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.
Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 5					
Раздел 1. Базовый аппарат и постулаты Тема 1. Кона и пространства состояний: гильбертовы пространства, векторы состояния (кубиты) и сфера Блоха. Тема 2. Постулаты квантовой механики: операторы, измерения фон Неймана и проекционные измерения. Тема 3. Тензорные произведения: описание систем из нескольких кубитов и запутанность (энтанглемент)	8	8			19
Раздел 2. Квантовые логические элементы и схемы Тема 1. Однокубитные вентили: матрицы Паули, вентили Адамара, фазовые вентили. Тема 2. Многокубитные вентили: управляемое отрицание (CNOT), вентиль Тоффли. Тема 3. Универсальность квантовых схем: теорема об универсальном наборе вентилей.	9	9			19
Итого в семестре:	17	17			38
Семестр 6					
Раздел 3. Квантовые алгоритмы Тема 1. Алгоритмы Дойча — Джозфы и Саймона: демонстрация квантового превосходства на простых задачах. Тема 2. Алгоритм Шора: разложение чисел на множители и дискретное логарифмирование. Тема 3. Алгоритм Гровера: квантовый поиск по неструктурированной базе данных.	8	8			19

Раздел 4. Квантовая теория информации и сложность Тема 1. Квантовые шумы и каналы: матрицы плотности, операторы Крауса. Тема 2. Квантовая коррекция ошибок: базовые коды защиты от декогеренции. Тема 3. Теория квантовой сложности: классы BQP, QMA и их связь с классическими классами.	9	9			19
Итого в семестре:	17	17			38
Итого	34	34	0	0	76

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
Раздел 1. Базовый аппарат и постулаты Тема 1. Кона и пространства состояний: гильбертовы пространства, векторы состояния (кубиты) и сфера Блоха. Тема 2. Постулаты квантовой механики: операторы, измерения фон Неймана и проекционные измерения. Тема 3. Тензорные произведения: описание систем из нескольких кубитов и запутанность (энтанглемент)	Кубиты и сфера Блоха: описание квантового бита как вектора в двумерном комплексном пространстве. Геометрическое представление чистых состояний кубита точками на единичной трехмерной сфере. Постулаты квантовой механики: правила эволюции закрытых систем с помощью унитарных операторов и математическое описание измерения. Вероятность исхода определяется квадратом модуля амплитуды (правило Борна). Многокубитные системы: использование тензорного произведения пространств для построения составных систем. Разделение состояний на сепарабельные и запутанные (например, состояния Белла), которые нельзя представить в виде произведения отдельных кубитов.
Раздел 2. Квантовые логические элементы и схемы Тема 1. Однокубитные вентили: матрицы Паули, вентили Адамара, фазовые вентили. Тема 2. Многокубитные вентили: управляемое отрицание (CNOT), вентиль Тоффоли. Тема 3. Универсальность квантовых схем: теорема	Однокубитные вентили: изучение матриц Паули, оператора Адамара, создающего суперпозицию, и фазовых сдвигов как поворотов на сфере Блоха. Многокубитные вентили: анализ обратимых логических элементов. Операция CNOT (управляемое НЕ) для генерации запутанности и трехкубитный вентиль Тоффоли (CCNOT) для реализации классической логики. Квантовые цепи и универсальность: правила сборки вентилей в квантовые схемы, где время идет слева направо. Доказательство того, что конечный набор вентилей (например, H, CNOT, T) может аппроксимировать любое унитарное преобразование с заданной точностью.

об универсальном наборе вентилей.	
Раздел 3. Квантовые алгоритмы Тема 1. Алгоритмы Дойча — Джозфы и Саймона: демонстрация квантового превосходства на простых задачах. Тема 2. Алгоритм Шора: разложение чисел на множители и дискретное логарифмирование. Тема 3. Алгоритм Гровера: квантовый поиск по неструктурированной базе данных.	Квантовые алгоритмы Квантовый параллелизм: концепция одновременного вычисления функции $f(x)$ для всех возможных аргументов x за один проход за счет суперпозиции. Субэкспоненциальные алгоритмы: разбор алгоритмов Дойча — Джозфы и Саймона, доказывающих экспоненциальный отрыв квантовых вычислений от классических в рамках оракульных задач. Алгоритм Шора: применение квантового преобразования Фурье (QFT) для поиска периода функции, что позволяет раскладывать целые числа на множители (факторизация) за полиномиальное время и взламывать криптосистемы RSA. Алгоритм Гровера: метод амплитудного усиления, позволяющий найти нужный элемент в неструктурированной базе данных из N элементов за время $O(\sqrt{N})$, что дает квадратичное ускорение по сравнению с классическим перебором $O(N)$.
Раздел 4. Квантовая теория информации и сложность Тема 1. Квантовые шумы и каналы: матрицы плотности, операторы Крауса. Тема 2. Квантовая коррекция ошибок: базовые коды защиты от декогеренции. Тема 3. Теория квантовой сложности: классы BQP, QMA и их связь с классическими классами.	Смешанные состояния: использование матриц плотности ρ для описания открытых квантовых систем, взаимодействующих с окружающей средой. Операторы Крауса для моделирования квантовых каналов связи и процессов декогеренции. Коррекция ошибок: математические методы защиты квантовой информации. Код Шора и поверхностные коды, которые позволяют исправлять ошибки переворота фазы (Z) и переворота бита (X) без разрушения самой суперпозиции. Квантовая сложность: определение класса BQP (задачи, решаемые на квантовом компьютере за полиномиальное время с малой вероятностью ошибки). Доказательство включений и изучение квантового аналога класса NP — класса QMA.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 5					
1	Геометрия кубита, тензорные произведения и квантовая запутанность	Семинар-практикум с элементами визуализации	8		1
2	Синтез квантовых цепей и проверка универсальности	Работа в визуальных симуляторах	9		2
Семестр 6					

3	Программирование квантовых алгоритмов Гровера и Дойча	Хакатон	8		3
4	Моделирование декогеренции и квантовая коррекция ошибок	Исследовательский семинар (Case Study)	9		4
Всего			34		

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час	Семестр 6, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)	40	20	20
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)	18	9	9
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)	18	9	9
Всего:	76	38	38

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8— Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
https://e.lanbook.com/book/426110 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Филиппов, Ф. В. Квантовые вычисления : учебное пособие / Ф. В. Филиппов. — Санкт- Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 83 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/426110 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/499784 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Филиппов, Ф. В. Квантовые вычисления на Python : учебное пособие / Ф. В. Филиппов. — Вологда : Инфра-Инженерия, 2025. — 108 с. — ISBN 978-5- 9729-2474-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/499784 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/426116 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Кирилук, М. А. Квантовые вычисления для решения задач искусственного интеллекта : учебное пособие / М. А. Кирилук, Н. А. Бочаров. — Москва : РТУ МИРЭА, 2026. — 95 с. — ISBN 978-5-7339-2874- 6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/523260	

	(дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/432662 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Сысоев, С. С. Введение в квантовые вычисления. Квантовые алгоритмы : учебное пособие / С. С. Сысоев. — Санкт-Петербург : СПбГУ, 2019. — 144 с. — ISBN 978-5-288- 05933-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/505514 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/505514 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Масленников, В. В. Введение в квантовые вычисления : учебное пособие / В. В. Масленников. — Москва : РТУ МИРЭА, 2024. — 74 с. — ISBN 978-5-7339-2254- 6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/432662 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/523260 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Филиппов, Ф. В. Квантовые вычисления: лабораторный практикум : учебное пособие / Ф. В. Филиппов. — Санкт- Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 42 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/426116 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	

7. Перечень электронных образовательных ресурсов
информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso
2	Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)
3	LibreOffice 5 (Лицензия LGPLv3)

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
1	Образовательная платформа «Юрайт» (https://urait.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru/), доступ через личный кабинет читателя библиотеки ГУАП

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
-------	---	-------------------------------------

1	Компьютерный класс	52-44 Большая Морская,67.
2	Аудитории для самостоятельной подготовки	14-34 Большая Морская,67
3	Лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Дифференцированный зачёт	Список вопросов; Тесты; Задачи.
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления;

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	Что такое кубит с математической точки зрения и чем его пространство состояний отличается от классического бита? Дайте определение чистых и смешанных квантовых состояний. В чем их математическое различие? Каков геометрический смысл сферы Блоха? Как на ней отображаются ортогональные состояния? Сформулируйте постулат квантовой механики, описывающий эволюцию изолированной квантовой системы. В чем различие между проекционными измерениями (фон Неймана) и общими квантовыми измерениями (POVM)? Сформулируйте правило Борна для расчета вероятностей исходов квантового измерения. Как математически строится пространство состояний многокубитной системы? Напишите формулу для трех кубитов. Дайте определение квантовой запутанности (энтанглемент). Приведите пример запутанного состояния. Сформулируйте и докажите критерий сепарабельности для двухкубитного состояния. Сформулируйте теорему о запрете клонирования (No-cloning theorem) и приведите ее математическое доказательство. Напишите матричные представления и опишите физический смысл однокубитных операторов Паули (X, Y,	ПК-3.3.1

	Z). Какую математическую трансформацию осуществляет оператор Адамара (H)? Напишите его матрицу. Опишите действие фазовых вентилей S и T. Каковы их матричные представления? Что такое управляемые вентили? Напишите матрицу оператора $CNOT$ и опишите его логику работы. Как с помощью вентилей H и $CNOT$ сгенерировать максимальное запутанное состояние (состояние Белла)? Опишите трехкубитный вентиль Тоффоли ($CCNOT$). Почему он важен для реализации классических обратимых вычислений? Что понимается под «универсальным набором квантовых вентилей»? Приведите пример такого набора. Сформулируйте суть теоремы Соловея — Китаева и ее значение для синтеза квантовых схем. Как графически отображаются квантовые схемы? Объясните назначение линий кубитов, классических битов и значков измерения. Что такое глубина квантовой схемы и размер квантовой схемы? Как эти параметры влияют на эффективность вычислений?	
2	В чем заключается математическая суть концепции квантового параллелизма? Какую роль в квантовых алгоритмах играет «оракул» (фазовый и разностный) и как он реализуется унитарным оператором? Опишите математическую постановку задачи и квантовый алгоритм Дойча. Какое преимущество он дает? В чем заключается обобщение алгоритма Дойча в рамках алгоритма Дойча — Джозфы? Опишите задачу Саймона и объясните, как его алгоритм демонстрирует экспоненциальный отрыв от классических алгоритмов. Какова математическая структура квантового преобразования Фурье (QFT)? Напишите его формулу. Опишите пошаговую схему алгоритма Шора. Какие шаги выполняются на классическом компьютере, а какие — на квантовом? Как алгоритм Шора сводит задачу факторизации чисел к задаче поиска периода функции? Опишите геометрический смысл алгоритма Гровера через повороты вектора состояния в двумерном подпространстве. Какова математическая функция оператора диффузии (амплитудного усиления) в алгоритме Гровера? Почему оптимум достигается за $(O\sqrt{N})$ шагов?	ПК-3.У.1
3	Что такое матрица плотности? Напишите ее свойства (след, эрмитовость, неотрицательная определенность). Как с помощью частичного следа (Partial Trace) получить состояние подсистемы из общего запутанного состояния? Опишите представление квантовых каналов через	ПК-3.В.1

	операторы Крауса (формализм операторов суперпозиции). Каковы математические модели шума деполяризации и шума фазового сдвига (Phase damping)? Опишите метрики расстояния между квантовыми состояниями: следственное расстояние (Trace distance) и верность (Fidelity). В чем главная сложность защиты квантовой информации от ошибок по сравнению с классической (с учетом теоремы о запрете клонирования)? Опишите математический принцип работы трехкубитного кода для исправления ошибки переворота бита (Bit-flip). Какова структура и принцип работы 9-кубитного кода Шора? От каких типов ошибок он защищает? Дайте определение класса сложности BQP. Какие известные задачи в него входят и как он соотносится с классами P и NP? Что такое класс сложности QMA? Опишите задачу «Локальный гамильтониан» как квантовый аналог задачи выполнимости (SAT).	
--	---	--

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	Вопрос 1 Какое базовое свойство геометрической модели кубита (сферы Блоха) отличает чистое квантовое состояние от смешанного? Правильный ответ: А А) Чистые состояния лежат строго на поверхности сферы, а смешанные — внутри нее Б) Чистые состояния лежат на экваторе сферы, а смешанные — на ее полюсах В) Смешанные состояния всегда находятся в центре сферы, а чистые — в любой другой точке Г) Никакого геометрического различия между ними на сфере Блоха нет Вопрос 2 Что происходит с запутанной системой из двух кубитов, если произвести полное физическое измерение только одного из них? Правильный ответ: В А) Измеренный кубит перейдет в случайное состояние, а второй останется полностью неизменным Б) Запутанность усилится, и кубиты обменяются своими	ПК-3.3.1

	начальными свойствами В) Измерение мгновенно определит состояние второго кубита, разрушив общую запутанность Г) Измерение одного кубита физически невозможно выполнить без одновременного измерения второго Вопрос 3 В чем заключается концептуальный смысл теоремы о запрете клонирования в квантовых вычислениях? Правильный ответ: Б А) Запрещено копировать данные с классического компьютера на квантовый Б) Невозможно создать идеальную копию неизвестного и изолированного квантового состояния В) Квантовые процессоры нельзя дублировать в кремниевых чипах Г) Один и тот же квантовый алгоритм нельзя запускать на выполнение дважды Разбор ответов Раздела 1 К вопросу 1: Любое чистое квантовое состояние представляется точкой на поверхности единичной сферы Блоха. Смешанные состояния (состояния с потерей когерентности или недостатком информации) графически отображаются точками внутри сферы, отражая уменьшение длины вектора состояния. К вопросу 2: Квантовая запутанность означает наличие неклассических корреляций. Физическое измерение одного кубита заставляет общую систему схлопнуться в один из базисных вариантов, из-за чего состояние второго кубита становится строго определенным, а сама связь (запутанность) исчезает. К вопросу 3: Из фундаментального принципа линейности квантовой механики следует, что не существует универсального физического процесса (вентилля), способного скопировать произвольное, заранее неизвестное состояние кубита, сохранив оригинал в исходном виде.	
2	Вопрос 4 Какой квантовый логический вентиль используется для перевода кубита из базового (строго определенного) состояния в состояние равновероятной суперпозиции? Правильный ответ: Б А) Вентиль Паули-Х (NOT) Б) Вентиль Адамара (H) В) Управляемое НЕ (CNOT) Г) Вентиль фазового сдвига (T) Вопрос 5 Какое действие выполняет двухкубитный логический вентиль CNOT (управляемое НЕ)? Правильный ответ: В А) Случайным образом меняет местами состояния обоих кубитов Б) Изменяет состояние первого кубита только в том случае, если второй равен нулю В) Изменяет состояние второго кубита на противоположное только тогда, когда первый кубит равен единице	ПК-3.У.1

	Г) Всегда инвертирует оба кубита одновременно Вопрос 6 Что такое глубина квантовой схемы (схемная глубина)? Правильный ответ: Б А) Общее физическое количество кубитов, задействованных в вычислительном процессе Б) Минимальное количество последовательных временных шагов, необходимых для выполнения всех вентилей В) Процент брака и ошибок при физическом изготовлении квантового процессора Г) Количество классических компьютеров, объединенных в сеть с квантовым симулятором Разбор ответов Раздела 2 К вопросу 4: Именно вентиль Адамара переводит «классические» состояния кубита (ноль или один) в суперпозиционные состояния, где шансы получить ноль или единицу при измерении равны 50 на 50. Это ключевой элемент для создания квантового параллелизма. К вопросу 5: Логика вентиля CNOT заключается в условном перевороте: первый кубит выполняет роль управляющего (контроллера). Если он находится в состоянии логической единицы, то состояние второго (целевого) кубита инвертируется (ноль меняется на единицу, а единица на ноль). К вопросу 6: Глубина схемы характеризует время работы алгоритма. Если некоторые вентили выполняются параллельно на разных кубитах, они занимают один шаг. Количество таких последовательных шагов (слоев вентилей) от начала цепи до измерения и называется глубиной.	
3	Вопрос 7 Какое принципиальное преимущество дает использование квантового параллелизма в алгоритмах? Правильный ответ: Б А) Возможность одновременно запускать программу на тысячах классических серверов Б) Способность обрабатывать суперпозицию всех возможных входных данных за один физический шаг В) Повышение тактовой частоты квантового процессора до бесконечности Г) Мгновенное стирание памяти без выделения тепла Вопрос 8 Какую практическую задачу позволяет решать алгоритм Шора, что делает его критически опасным для криптографических стандартов Интернета? Правильный ответ: Б А) Мгновенный подбор паролей методом полного перебора всех символов Б) Разложение огромных целых чисел на простые множители за реалистичное время В) Блокирование хакерских атак на базы данных за счет квантового шифрования Г) Прогнозирование курсов акций на финансовых биржах Вопрос 9	ПК-3.В.1

	В чем заключается суть работы алгоритма Гровера при поиске информации в неструктурированной базе данных? Правильный ответ: Б А) Он последовательно и очень быстро проверяет каждую запись по очереди Б) Он циклически увеличивает вероятность (амплитуду) правильного ответа, одновременно подавляя шум других записей В) Он автоматически сортирует базу данных по алфавиту за нулевое время Г) Он удаляет из базы данных все неверные ответы, оставляя только один нужный	
--	---	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Курс лекций разбивается на три последовательных логических модуля:

1. Фундаментальный (лекции 1–5): Перевод понятий классической информатики на язык квантовой механики и линейной алгебры.
2. Алгоритмический / Криптоаналитический (лекции 6–12): Изучение квантовых схем, принципа работы базовых алгоритмов и механизмов взлома классических шифров (Шора, Гровера).
3. Защитный / Инженерный (лекции 13–18): Изучение квантовой коммуникации (QKD), постквантовых криптосистем и стандартов безопасности.

Типовая структура одной лекции (План подачи материала)

Каждое лекционное занятие (стандартные 2 академических часа / 90 минут) жестко структурировано для обеспечения максимальной scannability (читаемости) и усвояемости:

1. Вводная часть (5–10 минут)

Тема и план лекции: Озвучивание ключевых вопросов.

Связь с предыдущим материалом: Краткое повторение (например, перед разбором алгоритма Шора кратко повторяется квантовое преобразование Фурье).

Мотивационный блок: Объяснение, какую конкретную проблему информационной безопасности решает данная тема.

2. Теоретическое / Математическое обоснование (25–30 минут)

Введение математического аппарата (векторы, матрицы, операторы).

Формулировка физических ограничений или постулатов квантовой механики, применимых к теме.

Алгоритмическая / Схемотехническая часть (30 минут)

Построение квантовой схемы: Разбор вентилей, их последовательности и принципа трансформации квантовых состояний.

Пошаговая трассировка: Разбор работы алгоритма на простом примере (например, для 2-3 кубитов).

Криптографический анализ и применение (15 минут)

Оценка защищенности: Как данный алгоритм влияет на стойкость шифров (RSA, AES) или как протокол защищает от перехвата.

Ресурсный анализ: Сколько кубитов и времени требуется для реализации (теория vs реальная практика).

Заключительная часть (5 минут)

Резюме (Выводы): Краткая фиксация главных тезисов лекции.

Анонс: Связь с темой следующей лекции и лабораторной работы.

Форма и методическое обеспечение лекционного материала

Лекционный материал предоставляется студентам в мультимедийном и текстовом виде:

Презентационные материалы (Слайды): Основной визуальный якорь. Содержат минимум сплошного текста, акцент делается на квантовые схемы, архитектурные диаграммы сетей QKD и графики.

Конспект лекций (Скрипт): Текстовое пособие, включающее строгие математические выводы, которые тяжело воспринимать со слайдов.

Интерактивные демонстрации: Использование преподавателем в процессе лекции визуализаторов (например, среды *Quirk* или *IBM Quantum Composer*) для демонстрации «живого» изменения состояний кубитов на сфере Блоха.

11.2. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимися практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Требования к проведению практических занятий

1. Инфраструктурные и программные требования

- Техническое оснащение: наличие персонального компьютера с доступом в интернет для каждого студента. Квантовые вычисления моделируются локально или через облачные сервисы.
- Программная среда: предустановленный интерпретатор Python 3.10+ и среда разработки Jupyter Notebook или VS Code.
- Квантовые библиотеки: обязательное наличие актуальных версий библиотек Qiskit (IBM) или Cirq (Google) для написания кода.
- Облачный доступ: зарегистрированные учебные аккаунты на платформе IBM Quantum Platform для доступа к реальным квантовым процессорам (по возможности) и графическому конструктору Composer.
- Инструменты визуализации: доступ к веб-симулятору Quirk для быстрой прототипичной проверки схем без написания кода.

2. Методические требования к структуре занятия

Каждое практическое занятие длительностью 2 академических часа должно состоять из трех обязательных этапов:

Входной контроль и теория (15–20 минут): экспресс-опрос или аналитический разбор математической базы на доске. Студенты должны доказать понимание линейной алгебры (матриц, векторов, тензорных произведений) до начала работы на ПК.

Самостоятельное программирование (50–60 минут): выполнение практического задания по написанию квантового алгоритма или сборке схемы. Преподаватель выступает в роли ментора, помогая с отладкой квантовой логики.

Защита результатов (10–15 минут): демонстрация работающего кода, объяснение гистограмм распределения вероятностей или расчетных матриц плотности.

Требования к оформлению и результатам (KPI студента)

По итогам каждого занятия студент обязан предоставить отчет, содержащий:

Математический расчет: аналитический вывод формул, векторов состояний или матриц операторов, использованных в работе.

Файл кода: работающий скрипт в формате .ipynb (Jupyter) с подробными комментариями к каждому квантовому регистру и вентилю.

Графический анализ: скриншоты или графики (сфера Блоха, гистограммы измерений, схемы цепей) с интерпретацией полученных результатов.

Анализ ошибок: при моделировании шумов — расчет метрики Fidelity (верности состояния) до и после применения кодов коррекции.

Критерии оценивания

Практические работы оцениваются по многофакторной шкале:

Корректность математической модели: правильность аналитических вычислений и понимание постулатов (критерий: 30% оценки).

Работоспособность кода/схемы: отсутствие синтаксических и логических ошибок в квантовых цепях (критерий: 40% оценки).

Глубина анализа: умение объяснить, почему алгоритм дает именно такое распределение вероятностей при измерении (критерий: 20% оценки).

Защита работы: устные ответы на контрольные вопросы по теме занятия (критерий: 10% оценки).

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Выполнение практических работ (40%): Разработка квантовых схем и программного кода, оформление и своевременная защита отчетов.

Контрольные работы / Тестирование (30%): Сдача промежуточных тестов по теории квантовой информатики и квантового криптоанализа.

Самостоятельная работа и активность на семинарах (20%): Решение практических задач у доски, разбор кейсов, подготовка докладов по современным стандартам постквантовой криптографии.

Посещаемость и ведение конспектов (10%): Регулярное присутствие на лекционных и практических занятиях.

Формы контроля и методические рекомендации по сдаче

Защита лабораторных работ

Сроки: Работа должна быть сдана в течение 1–2 недель после ее проведения по графику. За несвоевременную сдачу (без уважительной причины) рейтинг снижается на 20–50%.

Процедура: Студент демонстрирует преподавателю работающий код (в среде Qiskit/Jupyter) или схему, предоставляет отчет и устно отвечает на 2–3 контрольных вопроса.

Совет обучающемуся: Перед защитой повторите физический смысл используемых вентилей (например, зачем нужен вентиль Адамара в вашей схеме) и умейте объяснить каждую строчку своего кода.

Промежуточное тестирование (Текущие тесты)

Формат: Компьютерное или письменное тестирование по завершении крупных разделов (например, после Модуля 3 «Квантовый криптоанализ»).

Условия: Тест содержит 10–15 вопросов с ограничением по времени (в среднем 1.5–2 минуты на вопрос). Повторные попытки для повышения оценки обычно не предоставляются.

Совет обучающемуся: Обратите внимание на базовые понятия (свойства кубитов, отличия алгоритма Шора от Гровера, математические основы постквантовой криптографии). Тесты проверяют понимание сути процессов, а не заучивание сложных формул.

Контрольная работа (Решение задач)

Формат: Письменное решение практических задач (например, расчет выходного состояния квантовой схемы после прохождения вентилей Паули, или расчет уровня ошибок в протоколе BB84 при определенном типе атаки).

Совет обучающемуся: Тщательно расписывайте ход решения. Преподаватель оценивает логику рассуждений, даже если в финальном арифметическом расчете допущена ошибка.

Шкала оценивания и условия допуска к зачету

По итогам текущего контроля формируется семестровый рейтинг студента:

от 85 до 100 баллов — оценка «Отлично» (высокий уровень компетенций, возможен автоматический зачет).

от 71 до 84 баллов — оценка «Хорошо» (средний уровень, стабильная работа в семестре).

от 51 до 70 баллов — оценка «Удовлетворительно» (минимально допустимый уровень знаний).

менее 51 балла — оценка «Неудовлетворительно» (студент не освоил программу).

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Условия допуска к зачету

- Для получения допуска к промежуточной аттестации студент должен выполнить обязательный минимум учебной программы в семестре:
- Лабораторный практикум: Выполнить, оформить и успешно защитить все 5 лабораторных работ.

- Текущий контроль: Набрать по результатам текущего контроля успеваемости (балльно-рейтинговой системы) не менее 51 балла.
- При наличии академических задолженностей по лабораторным работам студент обязан ликвидировать их до начала зачетной сессии в дни консультаций преподавателя.

Формат и процедура проведения зачета

Зачет проводится в устно-письменной или тестовой форме по утвержденным вопросам (билетам):

1. Получение задания: Студент получает зачетный билет, который стандартно включает два теоретических вопроса (из разных разделов курса) и одно практическое задание (например, расчет состояния кубита после вентиля или анализ схемы).
2. Время на подготовку: На написание развернутого плана ответа и решение задачи студенту предоставляется 45 минут.
3. Использование материалов: Во время зачета категорически запрещено использование мобильных телефонов, шпаргалок, конспектов и сети Интернет. Допускается использование простой канцелярии.
4. Собеседование: Преподаватель выслушивает ответ студента по билету и может задать до 2–3 дополнительных или уточняющих вопросов в рамках программы дисциплины.

Критерии оценивания ответа студента

По результатам промежуточной аттестации выставляется бинарная оценка: «зачтено» или «не зачтено».

Оценка «Зачтено» выставляется, если студент:

Демонстрирует знание физико-математических основ квантовой информатики.

Понимает принципы работы алгоритмов Шора и Гровера, может объяснить характер их угроз для RSA, ECC и AES.

Свободно ориентируется в механизмах квантового распределения ключей (протоколы BB84, E91) и методах постквантовой защиты.

Успешно решил практическую задачу из билета или допустил в ней незначительную вычислительную ошибку, не нарушив логику квантовых преобразований.

Оценка «Не зачтено» выставляется, если студент:

Не может дать определения базовым понятиям (кубит, суперпозиция, квантовый вентиль).

Не понимает разницы между квантовым распределением ключей (физическая защита) и постквантовой криптографией (математическая защита).

Не справился с теоретическими вопросами билета и не смог ответить на наводящие вопросы преподавателя.

Нарушил правила проведения аттестации (использовал скрытые шпаргалки или технические средства).

Рекомендации по подготовке к зачету

Систематизация материала: Разделите вопросы к зачету на 4 смысловых блока (база, схемы, угрозы, защита) и повторяйте их последовательно.

Акцент на суть алгоритмов: Не зазубривайте сложные многомерные матрицы. Гораздо важнее понимать логику: какой вентиль создает суперпозицию (Адамар), какой связывает кубиты (CNOT), и почему алгоритм Шора работает быстрее классического перебора (за счет поиска периода функции через квантовое преобразование Фурье).

Повторение лабораторных: Просмотрите свои отчеты по лабораторным работам — практическая задача в билете часто дублирует элементы программного кода или расчетные таблицы из ваших работ.

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой