Аннотация

Дисциплина «Основы квантовых алгоритмов в защите информации» 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 разработкой и анализом 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 (7 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 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 оценки квантовых угроз современным шифрам 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.З.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:

- «Криптографические протоколы»,
- «Методы и средства криптографической защиты 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
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	17	17

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

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)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 7					
Раздел 1. Введение в квантовую информатику и физические основы Тема 1.1. Математический аппарат квантовых вычислений: гильбертовы пространства, матрицы плотности, бра-кет нотация Дирака. Тема 1.2. Квантовый бит (кубит) и его геометрическое представление (сфера Блоха). Тема 1.3. Фундаментальные свойства квантовых систем: суперпозиция, квантовая запутанность (сцепленность) и теорема о запрете клонирования. Тема 1.4. Измерения в квантовых системах: проективные измерения и их влияние на состояние кубита	2		2		6
Раздел 2. Квантовые схемы и базовые алгоритмы Тема 2.1. Квантовые логические вентили (Gates): однокубитные (X, Y, Z, H, фазовые сдвиги) и двухкубитные (CNOT, SWAP). Тема 2.2. Понятие квантовой схемы и обратимых вычислений. Универсальные наборы вентилей. Тема 2.3. Ранние квантовые алгоритмы: алгоритм Дойча-Йожи и алгоритм Саймона. Тема 2.3. Квантовое преобразование Фурье (QFT) и алгоритм оценки фазы	3		3		8

Раздел 3. Квантовый криптоанализ (Квантовые угрозы) Тема 3.1. Квантовый алгоритм Питера Шора: факторизация целых чисел и взлом криптосистемы RSA. Тема 3.2. Алгоритм Шора для дискретного логарифмирования: уязвимость протокола Диффи-Хеллмана и эллиптических кривых (ECC). Тема 3.3. Квантовый алгоритм поиска Лова Гровера: ускорение перебора и его влияние на симметричное шифрование (AES) и хеш-функции (SHA). Тема 3.4. Оценка реальных сроков и необходимых ресурсов (физических/логических кубитов) для реализации криптоанализа	4		4		8
Раздел 4. Квантовая криптография и квантовые коммуникации Тема 4.1. Квантовое распределение ключей (QKD): теоретическая безопасность на основе законов физики. Тема 4.2. Протоколы распределения ключей на одиночных фотонах: BB84 и B92. Анализ безопасности при наличии шума. Тема 4.3. Протоколы на основе запутанных состояний: протокол Экерта (E91). Тема 4.4. Квантовая телепортация и квантовые повторители для магистральных сетей связи.	4		4		8
Раздел 5. Постквантовая криптография и стандартизация Тема 5.1. Концепция постквантовой криптографии: математические альтернативы для классических ЭВМ. Тема 5.2. Криптография на решетках (Lattice-based cryptography) и кодовая криптография (Code-based). Тема 5.3. Криптография на многочленах (Multivariate) и на основе хеш-функций (Hash-based signatures). Тема 5.4. Современное состояние стандартизации постквантовых алгоритмов (стандарты NIST, рекомендации НКЦКИ/Технических комитетов).	4		4		8
Итого в семестре:	17		17		38
Итого	17	0	17	0	38

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. Введение в квантовую информатику и физические основы Тема 1.1. Математический аппарат квантовых вычислений: гильбертовы пространства, матрицы плотности, бра-кет нотация Дирака. Тема 1.2. Квантовый бит (кубит) и его геометрическое представление (сфера Блоха). Тема 1.3. Фундаментальные свойства квантовых систем: суперпозиция, квантовая запутанность (сцепленность) и теорема о запрете клонирования. Тема 1.4. Измерения в квантовых системах: проективные измерения и их влияние на состояние кубита	Изучаются базовые концепции квантовой механики, необходимые для понимания ИТ-технологий будущего. Рассматривается математический аппарат линейной алгебры, операции со сложными векторами и матрицами. Студенты осваивают понятия суперпозиции, когда кубит находится в нескольких состояниях одновременно, и квантовой запутанности, связывающей частицы на расстоянии. Демонстрируется теорема о запрете клонирования, которая делает невозможным незаметное копирование квантовой информации.
Раздел 2. Квантовые схемы и базовые алгоритмы Тема 2.1. Квантовые логические вентили (Gates): однокубитные (X, Y, Z, H, фазовые сдвиги) и двухкубитные (CNOT, SWAP). Тема 2.2. Понятие квантовой схемы и обратимых вычислений. Универсальные наборы вентилей. Тема 2.3. Ранние квантовые алгоритмы: алгоритм Дойча-Йожи и алгоритм Саймона. Тема 2.3. Квантовое преобразование Фурье (QFT) и алгоритм оценки фазы	Раздел посвящен архитектуре квантовых вычислений. Рассматриваются элементарные логические операции (вентили) над кубитами и правила построения квантовых схем. Студенты изучают базовые демонстрационные алгоритмы (Дойча-Йожи, Саймона), которые доказывают превосходство квантовых компьютеров над классическими. Особое внимание уделяется квантовому преобразованию Фурье как ключевому инструменту для ускорения сложных математических расчетов.
Раздел 3. Квантовый криптоанализ (Квантовые угрозы) Тема 3.1. Квантовый алгоритм Питера Шора: факторизация целых чисел и взлом криптосистемы RSA. Тема 3.2. Алгоритм Шора для дискретного логарифмирования: уязвимость протокола Диффи-Хеллмана и эллиптических кривых (ECC). Тема 3.3. Квантовый алгоритм поиска Лова Гровера: ускорение перебора и его влияние на симметричное шифрование (AES) и хеш-функции (SHA). Тема 3.4. Оценка реальных сроков и необходимых ресурсов (физических/логических кубитов) для реализации криптоанализа	Анализируется разрушительный потенциал квантовых вычислений для современной информационной безопасности. Подробно разбирается алгоритм Шора, способный за короткое время взламывать асимметричные шифры (RSA, ECC, Диффи-Хеллман), на которых держится безопасность интернета и банковских транзакций. Также изучается алгоритм Гровера, который ускоряет подбор ключей для симметричного шифрования (AES) и требует увеличения длины ключей в два раза

Раздел 4. Квантовая криптография и квантовые коммуникации Тема 4.1. Квантовое распределение ключей (QKD): теоретическая безопасность на основе законов физики. Тема 4.2. Протоколы распределения ключей на одиночных фотонах: BB84 и B92. Анализ безопасности при наличии шума. Тема 4.3. Протоколы на основе запутанных состояний: протокол Экерта (E91). Тема 4.4. Квантовая телепортация и квантовые повторители для магистральных сетей связи.	Изучаются методы защиты данных, основанные не на математических допущениях, а на фундаментальных законах физики. Центральное место занимает квантовое распределение ключей (QKD). На примере протоколов BB84 и E91 рассматривается, как любая попытка злоумышленника перехватить ключ неизбежно искажает квантовые состояния фотонов и обнаруживает присутствие шпиона. Разбираются принципы квантовой телепортации и построения защищенных сетей.
Раздел 5. Постквантовая криптография и стандартизация Тема 5.1. Концепция постквантовой криптографии: математические альтернативы для классических ЭВМ. Тема 5.2. Криптография на решетках (Lattice-based cryptography) и кодовая криптография (Code-based). Тема 5.3. Криптография на многочленах (Multivariate) и на основе хеш-функций (Hash-based signatures). Тема 5.4. Современное состояние стандартизации постквантовых алгоритмов (стандарты NIST, рекомендации НКЦКИ/Технических комитетов).	Раздел посвящен методам защиты информации, которые можно внедрять на существующих компьютерах уже сегодня для защиты от будущих квантовых угроз. Рассматриваются новые математические классы задач (криптография на решетках, кодах, хеш-функциях), которые одинаково сложны для взламывания как обычными, так и квантовыми процессорами. Изучается текущий статус международной и национальной стандартизации этих алгоритмов для перехода на новые защищенные протоколы.

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
Учебным планом не предусмотрено					
Всего					

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
Семестр 7				

1	Лабораторная работа №1: «Моделирование состояний одиночных кубитов и их визуализация на сфере Блоха»	2		1
2	Лабораторная работа №2: «Проектирование квантовых схем и программная реализация алгоритма Дойча-Йожи»	3		2
3	Лабораторная работа №3: «Исследование квантовых угроз: оценка уязвимости классических шифров перед алгоритмами Шора и Гровера»	4		3
4	Лабораторная работа №4: «Моделирование протокола квантового распределения ключей BB84 и симуляция атак перехвата»	4		4
5	Лабораторная работа №5: «Программная реализация и оценка производительности алгоритмов постквантовой криптографии»	4		5
	Всего	17		

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 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	9	9
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	9	9
Всего:	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.	Кирилюк, М. А. Квантовые вычисления для решения задач искусственного интеллекта : учебное пособие / М. А. Кирилюк, 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 средствдля 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
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; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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	1. Понятие кубита как базовой единицы квантовой информации. Геометрическое представление кубита на сфере Блоха. 2. Принцип квантовой суперпозиции и его отличие от классического вероятностного состояния. 3. Феномен квантовой запутанности (entanglement). Состояния Белла и их математическое описание. 4. Физический смысл теоремы о запрете клонирования (no-cloning theorem) и ее значение для информационной безопасности. 5. Математический аппарат квантовой механики: бра-кет нотация Дирака, векторы состояний и унитарные матрицы операторов. 6. Операция квантового измерения (проективное измерение) и эффект коллапса волновой функции при попытке съема данных. 7. Базовые однокубитные квантовые вентили (Паули X, Y, Z, оператор Адамара H, фазовые сдвиги) и их матрицы. 8. Двухкубитные вентили (оператор контролируемого НЕ — CNOT, вентиль SWAP) и создание запутанных состояний с их помощью. 9. Понятие обратимых вычислений в квантовых схемах. Универсальные наборы квантовых вентилей. 10. Алгоритм Дойча-Йожи: постановка задачи, структура квантовой схемы и демонстрация квантового превосходства. 11. Квантовое преобразование Фурье (QFT): назначение, математическая суть и роль в сложных квантовых алгоритмах.	ПК-3.З.1
2	Квантовый криптоанализ (Квантовые угрозы) 12. Алгоритм Питера Шора: общая схема работы, роль квантового поиска периода функции и угроза для	ПК-3.У.1

	криптосистемы RSA. 13. Уязвимость протоколов на основе дискретного логарифмирования (Диффи-Хеллман, ECC) перед модификациями алгоритма Шора. 14. Алгоритм Лова Гровера: принцип квантовой амплитудной амплификации и оценка ускорения перебора. 15. Влияние алгоритма Гровера на стойкость симметричных шифров (AES) и криптографических хеш-функций (SHA). Способы противодействия. 16. Ресурсный анализ квантового криптоанализа: разница между физическими и логическими кубитами, проблема квантовой коррекции ошибок.	
3	17. Квантовое распределение ключей (QKD): фундаментальное отличие от классического распределения ключей, роль законов физики. 18. Протокол квантового распределения ключей BB84: этапы формирования легитимного ключа, кодирование в базисах поляризации фотонов. 19. Моделирование атак злоумышленника (Евы) на протокол BB84: стратегия «измерение — повторная посылка» (intercept-resend) и механизм ее обнаружения. 20. Концепция постквантовой криптографии: определение, принципиальное отличие от квантовой криптографии. 21. Основные математические направления постквантовой криптографии (на криптографии на решетках, кодах, хеш-функциях) и текущий статус их мировой и отечественной стандартизации.	ПК-3.В.1

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. Как называется базовая единица квантовой информации, способная находиться в состоянии суперпозиции? А) Бит Б) Кубит В) Трит Г) Нанобит Правильный ответ: Б (Кубит) Вопрос 2. Какое свойство квантовых систем делает невозможным создание точной копии неизвестного квантового состояния для скрытого перехвата данных? А) Квантовая запутанность	ПК-3.З.1

	Б) Теорема о запрете клонирования В) Принцип неопределенности Гейзенберга Г) Декогеренция Правильный ответ: Б (Теорема о запрете клонирования) Вопрос 3. Что происходит с кубитом, находящимся в состоянии суперпозиции, в момент его измерения классическим прибором? А) Он переходит в состояние еще большей запутанности Б) Его состояние никак не изменяется В) Происходит коллапс волновой функции, и кубит случайно принимает одно из базовых состояний Г) Кубит полностью уничтожается без возможности считывания информации Правильный ответ: В (Происходит коллапс волновой функции, и кубит случайно принимает одно из базовых состояний) Вопрос 4. Какой квантовый логический вентиль является аналогом классического инвертора (НЕ) и осуществляет переворот бита? А) Вентиль Адамара (H) Б) Вентиль Паули-X В) Вентиль Паули-Z Г) Вентиль контролируемого НЕ (CNOT) Правильный ответ: Б (Вентиль Паули-X) Вопрос 5. Для чего используется квантовый вентиль Адамара (H)? А) Для изменения фазы кубита без изменения его значений Б) Для перевода кубита из базового состояния в состояние равной суперпозиции В) Для связывания двух кубитов в запутанное состояние Г) Для стирания квантовой информации Правильный ответ: Б (Для перевода кубита из базового состояния в состояние равной суперпозиции) Вопрос 6. Какое свойство является обязательным для всех квантовых вентилей и схем в силу законов квантовой механики? А) Необратимость Б) Обратимость (унитарность) В) Избыточность Г) Постоянная потеря энергии Правильный ответ: Б (Обратимость)	
2	Вопрос 7. Какую главную угрозу представляет алгоритм Шора для современной классической криптографии? А) Он позволяет за секунды подбирать пароли любой длины Б) Он эффективно решает задачи факторизации чисел и дискретного логарифмирования, взламывая RSA и ECC В) Он полностью дешифрует симметричный алгоритм AES без знания ключа Г) Он блокирует работу интернет-провайдеров на аппаратном уровне Правильный ответ: Б (Он эффективно решает задачи факторизации чисел и дискретного логарифмирования, взламывая RSA и ECC) Вопрос 8. Какое ускорение предоставляет алгоритм Гровера при поиске ключа в неупорядоченной базе данных по сравнению с классическим перебором? А) Экспоненциальное	ПК-3.У.1

	Б) Квадратичное В) Линейное Г) Алгоритм Гровера не дает ускорения Правильный ответ: Б (Квадратичное) Вопрос 9. Каким образом необходимо изменить параметры симметричного шифрования (например, AES), чтобы защитить его от атаки с применением алгоритма Гровера? А) Перейти на асимметричные ключи Б) Увеличить длину ключа в два раза (например, с AES-128 до AES-256) В) Снизить скорость шифрования данных Г) Использовать динамические IP-адреса Правильный ответ: Б (Увеличить длину ключа в два раза) Вопрос 10. На чем основана гарантированная безопасность квантового распределения ключей (QKD)? А) На сложности математических задач, которые трудно решить на компьютере Б) На фундаментальных законах физики и квантовой механики В) На большой длине передаваемого пароля Г) На использовании секретных алгоритмов шифрования государственных ведомств Правильный ответ: Б (На фундаментальных законах физики и квантовой механики) Вопрос 11. Как легитимные пользователи (Алиса и Боб) узнают о том, что злоумышленник пытался перехватить информацию в протоколе BB84? А) Сеть автоматически отключается оператором связи Б) Из-за вмешательства шпиона увеличивается уровень ошибок при сверке контрольной части ключа В) Фотоны меняют свой цвет на красный Г) Злоумышленник обязан отправить уведомление о перехвате по правилам протокола Правильный ответ: Б (Из-за вмешательства шпиона увеличивается уровень ошибок при сверке контрольной части ключа)	
3	Вопрос 12. Какое явление используется в протоколе Экерта (E91) для безопасного распределения криптографических ключей? А) Квантовая телепортация Б) Квантовая запутанность (сцепленность состояний) В) Вынужденное излучение Г) Эффект Доплера Правильный ответ: Б (Квантовая запутанность) Вопрос 13. Что такое постквантовая криптография? А) Криптография, которая работает исключительно на квантовых компьютерах Б) Новые математические алгоритмы для обычных компьютеров, устойчивые к атакам как классических, так и квантовых ЭВМ В) Системы шифрования, созданные после официального закрытия проекта квантовых вычислений Г) Способ передачи данных с помощью лазерных лучей в	ПК-3.В.1

	космосе Правильный ответ: Б (Новые математические алгоритмы для обычных компьютеров, устойчивые к атакам как классических, так и квантовых ЭВМ) Вопрос 14. Какое из перечисленных математических направлений является наиболее перспективным и популярным в постквантовой криптографии? А) Криптография на основе теории чисел и простых векторов Б) Криптография на решетках (Lattice-based cryptography) В) Шифрование с помощью фрактальных уравнений Г) Классические тригонометрические преобразования Правильный ответ: Б (Криптография на решетках) Вопрос 15. Какая организация в мире первой начала масштабный процесс отбора и стандартизации постквантовых алгоритмов шифрования? А) IEEE (Институт инженеров электротехники и электроники) Б) NIST (Национальный институт стандартов и технологий США) В) ISO (Международная организация по стандартизации) Г) Роскомнадзор Правильный ответ: Б (NIST)	

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 выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Общие требования к проведению лабораторных работ

1. Формат выполнения: Самостоятельное написание программного кода (скриптов) или сборка квантовых схем по индивидуальному варианту.
2. Требования к программной среде: Использование актуальных библиотек квантового программирования (предпочтительно Python + Qiskit/Cirq). Код должен снабжаться комментариями, поясняющими назначение каждого квантового вентиля.
3. Критерии успешной защиты:
   - Наличие работающего кода/схемы, демонстрирующего корректный результат.
   - Оформленный текстовый отчет.
   - Устные ответы на контрольные вопросы по теме работы.
4. Состав отчета:
   - Титульный лист с указанием темы, ФИО студента и варианта.
   - Цель работы и краткие теоретические сведения.
   - Графическое изображение спроектированной квантовой схемы (сгенерированное кодом или конструктором).
   - Исходный код программы (или ссылка на репозиторий).
   - Результаты моделирования: гистограммы распределения вероятностей, матрицы плотности или логи (выводы) работы алгоритма.
   - Анализ результатов и итоговый вывод.

Пример развернутого задания: Лабораторная работа №4

Тема: Моделирование протокола квантового распределения ключей BB84 и симуляция атак перехвата.

1. Цель работы

Практическое изучение принципов квантовой криптографии, моделирование этапов формирования секретного ключа в протоколе BB84 и анализ влияния измерения квантового канала связи третьей стороной (злоумышленником) на уровень ошибок.

2. Задание для студента

Разработать программу (рекомендуется в Jupyter Notebook с использованием Qiskit), имитирующую трех участников процесса: Алису (отправитель), Боба (получатель) и Еву (перехватчик). Программа должна выполнять следующие шаги:

1. Генерация данных Алисой: Создать случайную битовую строку (не менее 32 бит) и случайную последовательность базисов для кодирования (прямолинейный или диагональный).
2. Кодирование: Сформировать квантовую схему, где каждый бит Алисы переводится в кубит и кодируется с помощью вентилей (например, отсутствие вентилей для прямолинейного базиса, вентиль Адамара для диагонального).
3. Моделирование атаки Евы (по вариантам):

Вариант А: Ева отсутствует (чистый канал).

Вариант Б: Ева перехватывает все кубиты, измеряет их в случайно выбранных базисах и отправляет Бобу новые кубиты в соответствии со своим результатом (атака Intercept-Resend).

4. Измерение Бобом: Боб выбирает свои случайные базисы и измеряет полученные кубиты.
5. Провеивание ключа (Sifting): Моделировать классический открытый канал. Алиса и Боб сравнивают свои базисы, отбрасывают несовпавшие биты и формируют сырой ключ.
6. Оценка уровня ошибок (Error Rate): Вычислить процент несовпавших бит в итоговом ключе между Алисой и Бобом.

3. Требования к результатам

Программа должна наглядно выводить в консоль или графический интерфейс таблицы вида:

БИТЫ АЛИСЫ | БАЗИС АЛИСЫ | БАЗИС ЕВЫ | РЕЗУЛЬТАТ ЕВЫ | БАЗИС БОБА | РЕЗУЛЬТАТ БОБА | СОВПАДЕНИЕ БАЗИСОВ (ДА/НЕТ)

Для *Варианта А* уровень ошибок (QBER) должен быть равен 0%.

Для *Варианта Б* студент должен математически и практически подтвердить, что вмешательство Евы поднимает уровень ошибок в совпавших базисах примерно до 25%, что гарантирует обнаружение шпиона.

Структура и форма отчета о лабораторной работе

Общие требования к оформлению

Формат файла: PDF или DOCX (рекомендуется сдавать в PDF для сохранения верстки).

Шрифт: Times New Roman, размер 12–14 пт, межстрочный интервал — 1.5.

Выравнивание: По ширине страницы, абзацный отступ (красная строка) — 1.25 см.

Нумерация страниц: Сквозная, по центру или справа внизу (титульный лист считается первым, но номер на нем не ставится).

Форма структуры отчета (по разделам)

Титульный лист

Наименование министерства и учебного заведения.

Наименование кафедры.

Крупный заголовок: ОТЧЕТ о лабораторной работе № [Номер].

Тема работы (например: *«Моделирование протокола квантового распределения ключей BB84»*).

Данные автора: ФИО студента, группа, номер варианта.

Данные проверяющего: ФИО преподавателя, ученая степень/должность.

Город и текущий год (например: Москва, 2026).

Цель работы

Краткая формулировка того, какие навыки и знания приобретаются (1–3 предложения).

Пример: «Изучить принципы квантовой криптографии и экспериментально оценить уровень ошибок в ключе при наличии перехватчика в канале связи».

Краткие теоретические сведения

Ключевые понятия, формулировки алгоритмов или физических законов, используемых в работе.

Описание используемого ПО (например, *«Моделирование производилось в среде Jupyter Notebook с использованием библиотеки IBM Qiskit версии...»*).

Важно: раздел должен быть лаконичным (1–1.5 страницы), копировать учебник целиком запрещено.

Индивидуальное задание (Вариант)

Точный текст задания в соответствии со своим вариантом.

Исходные параметры (например, длина генерируемой последовательности, тип атаки злоумышленника, используемый универсальный набор вентилей).

Описание хода выполнения работы

Пошаговое описание реализации алгоритма или сборки схемы.

Текстовые пояснения к архитектуре созданной квантовой цепи.

Программный код (Листинг)

Полный исходный код написанной программы.

Код оформляется моноширинным шрифтом (например, Courier New, 10 пт) с обязательными комментариями к ключевым строкам.

Результаты работы и их анализ

Графические материалы: скриншоты спроектированных квантовых схем, графики распределения вероятностей (гистограммы результатов измерения).

Таблицы с результатами работы (сравнение базисов, сгенерированные и итоговые ключи).

Математический расчет или текстовое объяснение полученных аномалий (например, почему уровень ошибок составил именно ~25%).

Выводы

Итог выполнения работы. Обязательно соотносится с поставленной целью.

Пример: «В ходе лабораторной работы был успешно симулирован протокол BB84. Экспериментально подтверждено, что атака типа Intercept-Resend неизбежно вносит 25% ошибок в проверенный ключ, что позволяет легитимным пользователям однозначно обнаружить присутствие Евы».

Ответы на контрольные вопросы

Письменные ответы на вопросы, указанные в методических указаниях к данной работе.

Требования к оформлению отчета о лабораторной работе

бщие параметры текста

Формат страницы: A4, книжная ориентация (альбомная допускается только для крупных таблиц или схем).

Поля страницы: левое — 30 мм (для подшивки), правое — 10 мм, верхнее и нижнее — 20 мм.

Шрифт основного текста: Times New Roman, размер — 14 пт (в таблицах допускается 12 пт).

Цвет шрифта: строго черный.

Межстрочный интервал: 1.5 (полуторный).

Выравнивание: по ширине страницы.

Абзацный отступ (красная строка): 1.25 см (одинаковый по всему документу).

Нумерация страниц и заголовков

Страницы: нумеруются арабскими цифрами по центру или справа внизу страницы. На титульном листе номер не ставится, но сам лист учитывается (введение/цель работы начнется со страницы 2).

Заголовки разделов: пишутся жирным шрифтом (например, 14 или 16 пт), выравниваются по левому краю или по центру. Перед заголовком и после него делается пустая строка.

Точка в конце: в конце заголовка (как раздела, так и подраздела) точка не ставится.

Оформление программного кода (Листингов)

Так как дисциплина связана с программированием квантовых алгоритмов (Qiskit/Python), к коду предъявляются особые требования:

Шрифт: строго моноширинный (например, Courier New или Consolas), размер — 10 или 12 пт.

Интервал в коде: допускается уменьшать до 1.0 (одинарный).

Форматирование: длинный код (более 1-2 страниц) необходимо выносить в приложение в конце отчета. В самом тексте оставляются только ключевые фрагменты.

Комментарии: код должен содержать краткие комментарии на русском языке, объясняющие назначение квантовых вентилей (например: # добавление вентиля Адамара для создания суперпозиции).

Оформление графических материалов и таблиц

Рисунки (схемы, скриншоты, гистограммы):

Каждый рисунок должен быть отцентрирован.

Под рисунком обязательна подпись по форме: *Рисунок 1 — Квантовая схема алгоритма Дойча*.

В тексте отчета обязательно должна быть ссылка на изображение (например: *«...как показано на рисунке 1»*).

Таблицы:

Название таблицы пишется над ней с выравниванием по левому краю по форме: *Таблица 1 — Результаты сравнения базисов*.

Все ячейки и заголовки столбцов должны быть четко зафиксированы, текст внутри таблицы выравнивается по центру или по левому краю.

Оформление формул

Если в теоретической части или анализе результатов используются формулы (например, описание квантовых состояний Белла):

Формулы должны быть набраны в стандартном редакторе формул (MS Equation или LaTeX) и выровнены по центру.

Справа от формулы в круглых скобках указывается ее порядковый номер: *(1)*.

Все переменные, впервые встречающиеся в формуле, должны быть расшифрованы сразу под ней в формате: *«где ψ — это...»*.

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 обучающихсяявляются:

– 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.

Структура текущего контроля и распределение баллов

Максимальная оценка за текущий контроль в семестре составляет 100 баллов (или 50/50 при разделении с зачетом/экзаменом). Баллы распределяются по следующим видам активности:

Выполнение лабораторных 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».

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 21 вопрос 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