Приложение к ОПОП «Безопасность и этика искусственного интеллекта»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

РАБОЧАЯ ПРОГРАММА

дисциплины

«КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КВАНТОВАЯ КРИПТОГРАФИЯ»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2023

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.ф.-м.н., доцент Левина А.Б.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ 02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИС
Общая трудоемкость (ЗЕТ)	3
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	34
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	52
Самостоятельная работа, включая часы на контроль (академ. часов)	56
Всего (академ. часов)	108
Вид промежуточной аттестации	
Дифф. зачет (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КВАНТОВАЯ КРИПТОГРАФИЯ»

Квантовые вычисления и квантовая криптография, в настоящее время, является одним из самых перспективных направлений современной криптографии и защиты информации. В связи с приближением эры квантовых компьютеров современные алгоритмы криптографии не смогут обеспечить тот уровень защиты, который он предоставляли ранее. В данном курсе рассматриваются основные принципы работы квантовых систем и рассматриваются принципы работы криптоалгоритмов, построенных для квантовых компьютеров.

SUBJECT SUMMARY

«QUANTUM COMPUTING AND QUANTUM CRYPTOGRAPHY»

Quantum computing and quantum cryptography is currently one of the most promising areas of modern cryptography and information security. Due to the approach of the era of quantum computers, modern cryptography algorithms will not be able to provide the level of protection that it provided earlier. This course discusses the basic principles of quantum systems and examines the principles of operation of cryptoalgorithms built for quantum computers.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Целью изучения дисциплины «Квантовые вычисления и квантовая криптография» являются углубление и расширение знаний в области новейших перспективных направлений в информационных технологиях, новых принципов кодирования, обработки и передачи информации и вычислений, основанных на квантовой физике и приобретение навыков их применения в профессиональной деятельности.

2. Основные задачи дисциплины:

1) изучить теоретические основы принципов квантовой криптографии и проведения квантовых вычислений;

2) развить практические навыки решения задач в области квантовой криптографии, применения современных методов для реализации квантовых вычислений;

3) сформировать представления о современных фундаментальных и прикладных проблемах квантовой криптографии, проблемах приложения различных методов для реализации квантовых вычислений.

3. Знания теоретические основы квантовой криптографии; основные базовые протоколы квантового распределения ключей; различные виды атак на квантовые системы, а также методов противодействия им; теоретические основы и принципы квантовых вычислений; технику эксперимента с индивидуальными квантовыми системами; возможные риски ошибок квантовых вычислений.

4. Умения использовать современные методы квантовой криптографии при решении профессиональных задач; анализировать схемы реализации квантовых логических операций и квантовых криптопротоколов; анализировать криптографическую стойкость систем по отношению к различным атакам на них; со-

здавать и внедрять систему оценки точности квантовых вычислений; изменять существующие квантовые алгоритмы с целью их модификации; осуществлять управление рисками в квантовых вычислениях, приводящее к минимизации ошибок вычислительного эксперимента.

5. Владения математическим аппаратом, необходимым для реализации квантовых криптопротоколов сложных инфокоммуникационных систем; анализировать схемы реализации квантовых логических операций и квантовых криптопротоколов; навыками решения практических задач в области защиты квантовых систем; методами оценки точности квантовых вычислений; основными квантовыми алгоритмами; методами измерения состояния квантовых систем.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Математические основания информатики»

2. «Криптография и криптографические протоколы»

и обеспечивает подготовку выпускной квалификационной работы.

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ПК-23	Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта
ПК-23.3	*Разрабатывает единые стандарты в области безопасности (в том числе отказоустойчивости) и совместимости программного обеспечения, эталонных архитектур вычислительных систем и программного обеспечения, а также определяет критерии сопоставления программного обеспечения и критерии эталонных открытых тестовых сред (условий) в целях улучшения качества и эффективности программного обеспечения технологий и систем искусственного интеллекта*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	ИКР, ач	СР, ач
1	Основы квантовой механики	8	4		15
2	Чистые и смешанные состояния	8	4		15
3	Основные квантовые алгоритмы	8	4		15
4	Квантовая криптография	10	5	1	11
	Итого, ач	34	17	1	56
	Из них ач на контроль	0	0	0	0
	Общая трудоемкость освоения, ач/зе	108/3			

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Основы квантовой механики	
2	Чистые и смешанные состояния	
3	Основные квантовые алгоритмы	
4	Квантовая криптография	

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. «Демонстрация коллапса волновой функции на примере опыта Юнга»	2
2. «Регистрация квантовых наблюдаемых величин»	2
3. «Применение теоремы Шмидта к проблеме очищения состояний реальной квантовой системы»	2
4. «Наблюдение явления квантовой запутанности»	2

Наименование практических занятий	Количество ауд. часов
5. «Осуществление передачи информации по квантовым каналам»	2
6. «Применение квантовых кодов коррекции ошибок при передаче информации по квантовым каналам»	2
7. «Изучение постквантовых криптографических алгоритмов»	5
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

1. Программная реализация квантового алгоритма Гровера (раздел № 3).
2. Программная реализация квантового алгоритма Шора (раздел № 3).
3. Программная реализация квантового алгоритма Дойча-Йожи (раздел № 3).
4. Программная реализация квантового протокола BB84 (раздел № 4).
5. Программная реализация квантового протокола B92 (раздел № 4).
6. Программная реализация квантового протокола «4+2» (раздел № 4).
7. Программная реализация квантового протокола SARG04 (раздел № 4).

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	25
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	5
Самостоятельное изучение разделов дисциплины	5
Выполнение домашних заданий, домашних контрольных работ	5
Подготовка к лабораторным работам, к практическим и семинарским занятиям	14
Подготовка к контрольным работам, коллоквиумам	0
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0

Текущая СРС	Примерная трудоемкость, ач
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	2
ИТОГО СРС	56

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Квантовые устройства [Текст] : лаб. практикум / С.А. Баруздин, К.П. Наумов, Н.И. Пестриков и др. ; под ред. К.П. Наумова ; СПб.ГЭТУ, 1993. -63 с.	197
2	Нильсен М. Квантовые вычисления и квантовая информация [Текст] / М. Нильсен, И. Чанг ; пер. с англ. под ред. М.Н. Вялого и П.М. Островского с предисл. К.А. Валиева, 2006. -822 с.	19
3	Дулин, Виктор Николаевич. Электронные и квантовые приборы СВЧ [Текст] : учеб. для радиотехн. специальностей вузов / В. Н. Дулин, 1972. -222, [2] с.	36
Дополнительная литература		
1	Молотков, Николай Яковлевич. Основы общей физики [Текст] : учеб. для вузов в обл. техники и технологии : [в 3 т.]. -(Тонкие наукоемкие технологии). Т.3 : Кристаллооптика. Квантовые явления. Атомная и ядерная физика, 2017. -323 с.	15
2	Методические указания к лабораторным работам по дисциплине ”Квантовые и оптоэлектронные приборы и устройства” [Текст] : учеб. пособие / Сост.: Е.А. Смирнов, В.В. Черниговский; СПб. гос. электротехн. ун-т им. В.И. Ульянова (Ленина), 1993. -31 с. с.	50

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	ЭБС «АРБУЗ»http://lib.omgtu.ru
2	Квантовые технологииhttps://openedu.ru/course/msu/QUANTUMTECH/
3	Квантовая криптографияhttp://sqi.cs.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Квантовые вычисления и квантовая криптография» предусмотрены следующие формы промежуточной аттестации: зачет с оценкой.

Зачет с оценкой

Оценка	Описание
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок теорем
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач.

Особенности допуска

Студенты допускаются на дифф. зачет при условии посещения ими лекционных и практических занятий (не менее 80%). Для допуска к дифф. зачету требуется набрать проходной балл не менее 60% при прохождении теста и иметь удовлетворительную оценку по результатам выполнения контрольной работы.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к дифф.зачету

№ п/п	Описание
1	Волновая функция.
2	Чистые состояния.
3	Смешанные состояния.
4	Кубиты.
5	Квантовые наблюдаемые.
6	Коллапс волновой функции.
7	Парадокс ЭПР
8	Явление квантовой запутанности.
9	Очищение состояний.
10	Теорема Шмидта.
11	Невозможность клонирования.
12	Квантовые вычисления.
13	Квантовый алгоритм Гровера.
14	Квантовый алгоритм Шора.
15	Квантовый алгоритм Дойча-Йожи.
16	Передача информации по квантовым каналам.
17	Квантовые коды коррекции ошибок.
18	Протокол квантового распределения ключей BB84.
19	Протокол квантового распределения ключей B92.
20	Протокол квантового распределения ключей «2+4».
21	Протокол квантового распределения ключей SARG04.
22	5. Понятие о постквантовой криптографии. 6. Постквантовые криптографические алгоритмы
23	Постквантовые криптографические алгоритмы

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Основы квантовой механики	
2		
3		Практическая работа
4	Чистые и смешанные состояния	
5		
6		Практическая работа
7	Основные квантовые алгоритмы	
8		
9		Практическая работа
10	Квантовая криптография	
11		
12		
13		
14		Практическая работа

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), по результатам которого студент получает допуск на экзамен.

на практических (семинарских) занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), по результатам которого студент получает допуск на экзамен.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях. Сдача практических заданий будет проходить в форме коллоквиумов на которых проводится защита отчетов по практическим работам.

Критерии оценивания работы студентов на коллоквиумах:

«отлично» - тема вопроса раскрыта полностью, студент свободно владеет материалом и отвечает на дополнительные вопросы по теме.

«хорошо» - тема раскрыта не полностью, студент свободно владеет материалом, отвечает на дополнительные вопросы с несущественными ошибками.

«удовлетворительно» - в ответе имеются существенные ошибки, студент не дает ответов на дополнительные вопросы;

«неудовлетворительно» - ответ отсутствует, не соответствует теме, содержит грубые ошибки.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, компьютер	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2 4) C/C++, Java, Python
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, компьютер	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2 4) C/C++, Java, Python
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА
1	14.02.2023	Программа актуальна, изменения не требуются	14.02.2023, протокол заседания УМК №2	доцент, к.ф.-м.н., доцент, А.Б. Левина	