МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«__20__» ____09____ 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Квантовые вычисления и квантовая криптография

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.ф.-м.н. (Зуев С.В.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«14» 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	**Знать** Текущее состояние и тенденции развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.
		ОПК-9.2 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития средств технической защиты информации	**Уметь** Решать профессиональные задачи с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.
		ОПК-9.3 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	**Владеть** Современными методами и средствами для решения задач профессиональной деятельности.
	ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	**Уметь** Анализировать современные криптографические протоколы, в том числе квантовые.
		ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	**Владеть** Методиками применения квантовых средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Данная компетенция формируется следующими дисциплинами.

№	Наименование дисциплины (модуля)
1.	Безопасность систем баз данных
2.	Безопасность операционных систем
3.	Безопасность сетей ЭВМ
4.	Квантовые вычисления и квантовая криптография
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

2. Компетенция ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Данная компетенция формируется следующими дисциплинами.

№	Наименования дисциплины
1.	Методы и средства криптографической защиты информации
2.	Математика криптографии
3.	Криптографические интерфейсы
4.	Квантовые вычисления и квантовая криптография
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единицы, 144 часа.

Форма промежуточной аттестации дифференцированный зачет

(экзамен, дифференцированный зачет, зачет)

Вид учебной работы	Всего часов	Семестр № 10
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	71	71
лекции	34	34
лабораторные	17	17
практические	17	17
групповые консультации в период теоретического обучения и промежуточной аттестации	3	3
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	73	73
Курсовой проект		
Курсовая работа		
Расчетно-графическое задание		
Индивидуальное домашнее задание		
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	73	73
Дифференцированный зачет	-	-

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем
Курс 5 Семестр 2

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа на подготовку к аудиторным
1.	Элементы квантовой механики: постулаты, бра-кет формализм, основные теоремы				
	Алгебраические структуры на CP^n. Постулаты квантовой механики. Фейнмановский формализм. Измерения. Спектральное и полярное разложения.	6	4	-	9
2.	Квантовые вычисления, квантовые компьютеры и их физическая реализация				
	Понятие кубита, вычисления на одном кубите. Многочастичные вычислительные системы. Запутанность, ЭПР парадокс. Физическая реализация квантовых вычислителей.	8	3	2	15
3.	Квантовые схемы и алгоритмы, квантовое программирование				
	Квантовые гейты. Алгоритмы Дойча, Дойча-Йожа, Гровера, Шора. Поиск периода функции. Задачи для квантового программирования. Сложность квантовых вычислений. Факторизация и дискретное логарифмирование.	8	4	6	18
4.	Квантовая информация и исправление квантовых ошибок				
	Исправление классических и фазовых ошибок. Код Шора. Коды Стина и симплектические коды.	6	4	5	16
5.	Квантовая криптография				
	Протоколы BB84 и B92. ЭПР-протокол. Квантовое распределение ключей. CSS-коды. Модифицированный протокол Ло-Чу.	6	2	4	15
	ВСЕГО	34	17	17	73

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического (семинарского) занятия	К-во часов	Самостоятельная работа на подготовку к аудиторным занятиям
семестр № 10				
1	Элементы квантовой механики: постулаты, бра-кет формализм, основные теоремы	Фейнмановский формализм. Измерения.	2	2
		Спектральное и полярное разложения	2	2
2	Квантовые вычисления, квантовые компьютеры и их физическая реализация	Вычисления на одном кубите. Многочастичные вычислительные системы	3	4
3	Квантовые схемы и алгоритмы, квантовое программирование	Алгоритмы Дойча, Дойча-Йожа, Гровера.	2	3
		Поиск периода функции, алгоритм Шора. Факторизация и дискретное логарифмирование	2	3
4	Квантовая информация и исправление квантовых ошибок	Код Шора. Коды Стина и симплектические коды.	4	5
5	Квантовая криптография	Квантовое распределение ключей.	2	3
		ИТОГО:	17	22
			ВСЕГО:	39

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	Самостоятельная работа на подготовку к аудиторным занятиям
семестр № 10				
1	Квантовые вычисления, квантовые компьютеры и их физическая реализация	Моделирование эволюции запутанных состояний	2	3
2	Квантовые схемы и алгоритмы, квантовое программирование	Исследование сложности вычислений в алгоритме Гровера	4	5
3		Вычисление периода периодической функции	2	2
4	Квантовая информация и	Исправление произвольных ошибок при передаче квантовых состояний	3	3
5		Построение симплектического кода	2	3

	исправление квантовых ошибок			
6	Квантовая криптография	Модифицированный протокол Ло-Чу и CSS-коды.	4	8
		ИТОГО:	34	24
			ВСЕГО:	58

4.4. Содержание курсового проекта/работы

Учебным планом не предусмотрены

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Учебным планом не предусмотрены.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1 Компетенция ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-9.1 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	Прием лабораторных работ, устный опрос, дифференцированный зачет
ОПК-9.2 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития средств технической защиты информации	Прием лабораторных работ, устный опрос, дифференцированный зачет
ОПК-9.3 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Прием лабораторных работ, устный опрос, дифференцированный зачет

2 Компетенция ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	Прием лабораторных работ, устный опрос, дифференцированный зачет
ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	Прием лабораторных работ, устный опрос, дифференцированный зачет

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для дифференцированного зачета

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Элементы квантовой механики: постулаты, бракет формализм, основные теоремы	1. Опишите как строится пространство состояний квантовой системы. 2. Первый и второй постулаты квантовой механики: их физический смысл и математическая реализация. 3. Третий постулат квантовой механики: виды измерений. 4. Четвертый постулат квантовой механики в терминах бра-кет формализма. 5. Осуществить сингулярное разложение заданного оператора. 6. Осуществить полярное разложение заданного оператора. 7. Расширяющие квантовые системы: определение и пример.
2	Квантовые вычисления, квантовые компьютеры и их физическая реализация	1. Теорема о разложении Шмидта. 2. Запутанные состояния, их связь с ЭПР-парадоксом. 3. Понятие кубита и квантового вычисления. 4. Привести пример вычисления в многочастичной квантовой системе. 5. Принцип действия оптического квантового компьютера. 6. Адиабатические квантовые вычисления. 7. Квантовый вычислитель на основе ЯМР. 8. Существующие в мире квантовые компьютеры и их особенности.
3	Квантовые схемы и алгоритмы, квантовое программирование	1. Преобразование Уолша-Адамара. 2. Простейшая квантовая схема: квантовая телепортация. 3. Алгоритм Дойча. 4. Алгоритм Дойча-Йожа. 5. Алгоритм Гровера. 6. Какова сложность вычислений в алгоритме Гровера и как ее посчитать? 7. Эмуляторы квантовых вычислений: принцип работы, примеры. 8. Квантовое преобразование Фурье. 9. Определение периода периодической функции. 10. Факторизация и дискретное логарифмирование. 11. Как посчитать сложность квантовых алгоритмов факторизации и дискретного логарифмирования?
4	Квантовая информация и исправление квантовых ошибок	1. Предмет квантовой теории информации. 2. Классические и квантовые коды, код Шора. 3. Теорема Соловея-Китаева. 4. Коды Стина. 5. Симплектические коды.

		6. CSS-коды
5	Квантовая криптография	1. Понятие квантовой криптографии и принцип работы. 2. Первые квантовые протоколы. 3. Физические принципы работы устройств квантовой связи. 4. Протоколы квантового обмена информацией. 5. Модифицированный протокол Ло-Чу 6. Российские средства квантовой криптографии: назначение, характеристики.

5.2.2. Перечень контрольных материалов для защиты курсового проекта/ курсовой работы

Учебным планом не предусмотрены.

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Наименование индикатора достижения компетенции	Типовые контрольные задания
ОПК-9.1 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий	Опишите применение алгоритма Гровера для решения задачи подбора паролей. Как можно противодействовать этому? Как квантовые вычисления могут помочь злоумышленнику в поиске уязвимостей в системе?
ОПК-9.2 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития средств технической защиты информации	Какие физические принципы используются в квантовых вычислениях? Какие средства технической защиты информации могут использовать квантово-механические эффекты?
ОПК-9.3 Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Опишите работу квантовой сети передачи данных. Какие имеются проблемы, мешающие распространению квантовых сетей? Опишите передачу квантовых состояний с помощью телепортации – нарушается ли принцип относительности Эйнштейна?
ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	Приведите пример использования квантовых вычислений для решения задачи криптоанализа RSA Каким образом с помощью квантовых вычислений решается задача криптоанализа криптосистемы DRSA
ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	Отечественные средства квантовой связи: их назначение, технические характеристики и стоимость.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме дифференцированного зачета используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминологии
	Знание основных законов и методов квантовых вычислений
	Знания о применимости методов квантовых вычислений и квантовой криптографии в сфере профессиональной деятельности
	Объем и полнота освоенного материала
	Знания отечественного программного и аппаратного обеспечения для квантовых вычислений и квантовой криптографии
Умения	Способность уместно и правильно применять терминологию
	Способность решать задачи методами, рассмотренными в курсе
	Способность выбирать устройства квантовой криптографии в соответствии с потребностями в защите информации
Навыки	Написание программного кода на эмуляторах квантовых вычислений
	Вычисление сложности квантового алгоритма или квантового протокола

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю ***знания***.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминологии	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных законов и методов квантовых вычислений	Не знает принципов и методов квантовых вычислений	Имеет неполные знания о принципах и методах квантовых вычислений	Проявляет достаточно полные знания о принципах и методах квантовых вычислений	Знает принципы и методы квантовых вычислений, а также современное состояние исследований в этой области
Знания о применимости методов квантовых вычислений и квантовой криптографии в сфере профессиональной деятельности	Не имеет представлений о применении квантовых методов в области информационной безопасности	Знает примеры применения квантовых методов в области информационной безопасности	Демонстрирует понимание применения квантовых методов в области информационной безопасности	Показывает полное понимание работы квантовых методов в профессиональной сфере, демонстрирует творческий подход
Объем и полнота освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины,

		усвоил его деталей		владеет дополнительными знаниями
Знания отечественного программного и аппаратного обеспечения для квантовых вычислений и квантовой криптографии	Не знает отечественного квантового аппаратного и программного обеспечения	Знает о существовании отечественного квантового аппаратного и программного обеспечения	Может назвать примеры и производителей отечественного квантового аппаратного и программного обеспечения	Знает не только продукты и производителей отечественного квантового аппаратного и программного обеспечения, но и тенденции дальнейших разработок

Оценка сформированности компетенций по показателю ***умения***.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Способность уместно и правильно применять терминологию	Не применяет терминологию или применяет ее неуместно	Применяет терминологию, но допускает и бытовое описание	Применяет терминологию везде, где это необходимо	Уверенно применяет терминологию и умеет, при необходимости, интерпретировать ее
Способность решать задачи методами, рассмотренными в курсе	Не может решить ни одной задачи	Решает только наиболее простые задачи	Решает все задачи, кроме повышенной сложности	Решает все задачи, в том числе, повышенной сложности
Способность выбирать устройства квантовой криптографии в соответствии с потребностями в защите информации	Не имеет представления о характеристиках устройств квантовой связи	Может перечислить названия характеристик устройств квантовой связи, но не знает диапазонов их значений	Осуществляет выбор устройств квантовой связи по диапазонам значений их характеристик	Свободно ориентируется в современных и перспективных характеристиках устройств квантовой связи

Оценка сформированности компетенций по показателю ***навыки***.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Написание программного кода на эмуляторах квантовых вычислений	Не может написать даже простой код ни на каком эмуляторе	Имеет навык написания простых квантовых программ	Пишет квантовые программы с любым числом регистров и с любыми гейтами	Пишет квантовые программы с любым числом регистров и с любыми гейтами, может модифицировать квантовые алгоритмы
Вычисление сложности квантового алгоритма или	Не может определить сложность	Определяет сложность только по квантовой схеме	Определяет сложность по квантовой схеме с	Определяет сложность по квантовой схеме с учетом сложности

квантового протокола	кантовых вычислений		учетом сложности построения гейтов	построения гейтов, может провести корректное сравнение с классическим алгоритмом

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Аудитория 425 ГУК	Компьютерный класс с выходом в интернет
2	Аудитория 430 ГУК	Компьютерный класс с выходом в интернет

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Операционная система Ubuntu 18	Свободно распространяемое ПО
2	Операционная система Linux Mint 20	Свободно распространяемое ПО

6.3. Перечень учебных изданий и учебно-методических материалов

1. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. - М.: Мир, 2006. - 824 с.
2. Кайе Ф. Введение в квантовые вычисления [Электронный ресурс]: учебное пособие / Кайе Ф. – Электронные текстовые данные. – Ижевск: Регулярная и хаотическая динамика, 2009. – 360 с. Режим доступа: http://www.iprbookshop.ru/16499.html — ЭБС «IPRbooks».
3. Прескилл Дж. Квантовая информация и квантовые вычисления. / Дж. Прескилл. – Ижевск: НИЦ Регулярная и хаотическая динамика, 2011. – 464 с.
4. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации – Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2007.
5. Стин Э. Квантовые вычисления : пер. с англ. / Э. Стин. - Ижевск : Регулярная и хаотическая динамика, 2000. - 112 с.
6. Имре Ш. Квантовые вычисления и связь. Инженерный подход / Ш. Имре, Ф. Балаж ; пер. с англ. А. А. Калачева [и др.] ; ред. В. В. Самарцев. - Москва : Физматлит, 2008. - 319 с.
7. Методические указания к практическим занятиям по курсу «Квантовые вычисления» / сост. С.В. Зуев. – Белгород: Изд-во БГТУ, 2015. – 51 с.
8. Перри Р. Элементарное введение в квантовые вычисления. / Р. Перри. – М.: Мир, 2006. – 208 с.
9. Китаев А. Классические и квантовые вычисления. / А. Китаев, А. Шень, М. Вялый. – М.: МЦНМО – ЧеРо, 1999. – 192 с.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Система квантовых вычислений МГУ: https://rcp.qotlabs.org/
2. Научная библиотека БГТУ им. В.Г. Шухова: http://ntb.bstu.ru/jirbis2/

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 20____ /20____ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «_ _»_____ 20___ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО