ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Институт естественных и точных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 03.02.2022

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П2.08.01 Квантовая криптография
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
профиль подготовки Математические методы обеспечения безопасности программных систем
форма обучения очная
кафедра-разработчик Прикладная математика и программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 03.02.2022

А. А. Замышляева

Разработчик программы,
к.экон.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Дрозин Д. А.
Пользователь: drozinda
Дата подписания: 03.02.2022

Д. А. Дрозин

СОГЛАСОВАНО

Руководитель образовательной программы
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 03.02.2022

А. А. Замышляева

Челябинск

1. Цели и задачи дисциплины

Целью освоения дисциплины является ознакомление студентов с математическими методами квантовых коммуникаций и криптографии: описания квантовых вычислительных цепей и схем, исследование их свойств. Задачи: - получение навыков по применению методов построения математических моделей теории информации и их применение в криптографии; - ознакомление студентов с современными результатами теории квантовых вычислений, а также современными проблемами стоящими перед этой дисциплиной.

Краткое содержание дисциплины

Дисциплина содержит в себе изучение следующих разделов: фундаментальные принципы квантовых вычислений, введение в квантовую механику и квантовые схемы.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-6 Способен использовать математические методы при проектировании и разработке алгоритмических и программных решений в области обеспечения безопасности и защиты программных систем.	Знает: элементы квантовой теории информации Имеет практический опыт: реализации квантовых криптографических алгоритмов

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Математические основы криптографии, Теория информации и кодирования, Ассемблер в задачах защиты информации, Криптографические методы защиты информации	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Ассемблер в задачах защиты информации	Знает: технологии исследования программных алгоритмов Умеет: выстраивать систему защиты программы Имеет практический опыт: программирования на языке ассемблер, дизассемблирования и отладки программ
Математические основы криптографии	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при создании криптографических спецификаций Имеет практический опыт:
Криптографические методы защиты информации	Знает: принципы построения криптографических

	алгоритмов, криптографические стандарты, основные подходы к реализации криптографических средств защиты информации Умеет: Имеет практический опыт: решения задач, связанных с распределением ключевой информации, шифрованием чувствительной информации и цифровой подписью сообщений
Теория информации и кодирования	Знает: способы формирования оптимальных кодов в системе передачи информации Умеет: Имеет практический опыт: оценки предельных возможностей информационных систем, оптимального кодирования и передачи сигналов

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	24	24
Самостоятельная работа (СРС)	53,75	53,75
с применением дистанционных образовательных технологий	0	
Подготовка к промежуточной аттестации	8,75	8.75
Подготовка к лекциям	45	45
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Фундаментальные принципы квантовых вычислений	20	8	0	12
2	Введение в квантовую механику	14	8	0	6
3	Введение в информатику. Квантовые схемы	14	8	0	6

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во

			часов
1	1	Глобальные перспективы, квантовые биты	2
2	1	Квантовые вычисления. Однокубитные элементы, многокубитные элементы	2
3	1	Квантовые алгоритмы	2
4	1	Экспериментальная обработка квантовой информации. Квантовая информация	2
5	2	Линейная алгебра. Постулаты квантовой механики	2
6	2	Сверхплотное кодирование. Оператор плоскости	2
7,8	2	Разложение Шмидта. Парадокс Энштейна-Подольского-Розена.	4
9	3	Вычислительные модели. Машина Тьюринга. Схемы	2
10	3	Анализ вычислительных задач	2
11	3	Квантовые алгоритмы. Операции на одном кубите. Условные операции	2
12	3	Универсальные квантовые элементы. Модель квантовых схем вычислений	2

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Анализ ведущих квантовых вычислительных центров	6
2	1	Разработка компьютерной программы расчета состояния кубита	6
3	2	Разработка компьютерной программы моделирующей основные квантовые элементы	6
4	3	Разработка компьютерной программы моделирования квантовых схем	6

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к промежуточной аттестации	Шень, А. Х. Классические и квантовые вычисления/ : учебное пособие / А. Х. Шень, М. Н. Вялый. — 2-е изд. — Москва : ИНТУИТ, 2016. — 273 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100617 (дата обращения: 03.02.2022). — Режим доступа: для авториз. пользователей.	8	8,75
Подготовка к лекциям	Шень, А. Х. Классические и квантовые вычисления/ : учебное пособие / А. Х. Шень, М. Н. Вялый. — 2-е изд. — Москва : ИНТУИТ, 2016. — 273 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100617 (дата обращения: 03.02.2022). — Режим	8	45

	доступа: для авториз. пользователей.		

6. Текущий контроль успеваемости, промежуточная аттестация

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	8	Текущий контроль	Анализ ведущих квантовых вычислительных центров	20	1	Если задание выполнено без ошибок, написан отчет в соответствии с требованиями, то выставляется 1 балл. Иначе 0 баллов.	зачет
2	8	Текущий контроль	Разработка компьютерной программы расчета состояния кубита	20	1	Если задание выполнено без ошибок, написан отчет в соответствии с требованиями, то выставляется 1 балл. Иначе 0 баллов.	зачет
3	8	Текущий контроль	Разработка компьютерной программы моделирующей основные квантовые элементы	20	1	Если задание выполнено без ошибок, написан отчет в соответствии с требованиями, то выставляется 1 балл. Иначе 0 баллов.	зачет
4	8	Текущий контроль	Разработка компьютерной программы моделирования квантовых схем	20	1	Если задание выполнено без ошибок, написан отчет в соответствии с требованиями, то выставляется 1 балл. Иначе 0 баллов.	зачет
5	8	Проме-жуточная аттестация	Ответ по билету	-	3	Если вопрос раскрыт полностью - 1 балл. Если вопрос раскрыт, но не полностью - 0.5 балла. Если вопрос не раскрыт - 0 баллов	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Контрольное мероприятие промежуточной аттестации является обязательным и проводится в смешанной форме - письменно-устной. Студенту выдается билет, содержащий 3 вопроса. На подготовку выделяется 1 час, после чего студент сдает работу в письменном виде. Затем проводится собеседование.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ПК-6	Знает: элементы квантовой теории информации	+	+	+	+	+
ПК-6	Имеет практический опыт: реализации квантовых криптографических алгоритмов	+	+	+	+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Методические требования к оформлению отчетов

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Методические требования к оформлению отчетов

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Шень, А. Х. Классические и квантовые вычисления/ : учебное пособие / А. Х. Шень, М. Н. Вялый. — 2-е изд. — Москва : ИНТУИТ, 2016. — 273 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100617 (дата обращения: 03.02.2022). — Режим доступа: для авториз. пользователей.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Душкин, Р. В. Квантовые вычисления и функциональное программирование / Р. В. Душкин. — Москва : ДМК Пресс, 2015. — 232 с. — ISBN 978-5-97060-275-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/97340 (дата обращения: 03.02.2022). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. -Visual Studio 2017 Community(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	332 (3б)	Компьютеры, доска, проектор
Лабораторные занятия	340 (3б)	Компьютеры, доска
Лабораторные занятия	332 (3б)	Компьютеры, доска