Рабочая программа дисциплины

1. Название дисциплины: Дискретные функции и их приложения в криптографии

2. Уровень высшего образования – магистратура

3. Направление подготовки: 03.04.02 Физика (магистратура)

4. Аннотация:

Курс «Квантовая теория информации» является профильной дисциплиной магистерской программы «Математические методы защиты информации». Дисциплина обеспечивает базовую подготовку студентов в области физики квантовой информации. Курс состоит из двух основных частей, рассматривающих, соответственно, физические основы квантовой информатики и основные сведения о квантовых вычислениях. В частности, в части курса, посвященной теории квантовой информации рассматривается различимость квантовых состояний, различные метрики на пространстве квантовых состояний, передача классической информации по квантовым каналам и граница Холево, передача квантовой информации по квантовым каналам связи, меры количества квантовой информации, энтропия фон Неймана и её свойства, перепутанность квантовых состояний, количественные меры перепутанности, ресурсная теория перепутанности, теория квантовых процессов и описание шумов в квантовых каналах, основы квантовой томографии состояний и процессов.

5. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся (указывается согласно рабочему плану):

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа, из которых 36 часа составляет контактная работа обучающегося с преподавателем (18 часов занятия лекционного типа, 16 часа занятия семинарского типа, 2 часа коллоквиумов), 36 часа составляет самостоятельная работа обучающегося.

6. Формируемые компетенции и входные требования для освоения дисциплины, предварительные условия:

НАЗВАНИЕ КОМПЕТЕНЦИЙ:

СПК-1 Способность свободно владеть профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений.

СПК-2 Способность к поиску, критическому анализу, обобщению и систематизации научной информации в области физики квантовых вычислений.

СПК-3 Способность организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Для того чтобы формирование данных компетенций было возможно, обучающийся, приступивший к освоению образовательной программы, должен:

- ЗНАТЬ*:* основные методы научно-исследовательской деятельности.
- УМЕТЬ*:* выделять и систематизировать основные идеи в научных текстах; критически оценивать любую поступающую информацию, вне зависимости от источника; избегать автоматического применения стандартных формул и приемов при решении задач.
- ВЛАДЕТЬ*:* навыками сбора, обработки, анализа и систематизации информации по теме исследования; навыками выбора методов и средств решения задач исследования.

Для освоения дисциплины необходимы знания и умения, приобретаемые в рамках курса «Линейная алгебра», «Теория вероятностей и математическая статистика», курса теоретической физики «Квантовая теория».

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий

Наименование и краткое содержание разделов и тем дисциплины, **форма промежуточной аттестации по дисциплине**	**Всего, часы**	В том числе						
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				**Самостоятельная работа обучающегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Учебные занятия, направленные на проведение текущего контроля успеваемости коллоквиумы, практические контрольные занятия и др.*	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п.	**Всего**
1. Основные сведения из классической теории информации Энтропия Шеннона, её основные свойства. Относительная энтропия, условная энтропия и взаимная информация. Неравенство обработки данных. Теорема кодирования Шеннона для канала без шума.	2	2			2	2 часа Решение задач на на основные понятия классической информации, доказательства свойств введенных на лекции величин.		2

2. Квантовая теория информации §1. Необходимые сведения из квантовой теории. Квантовые состояния, Гильбертово пространство. Эволюция квантовых состояний, картина Шрёдингера. Измерения, вероятности в квантовой теории, POVM-формализм, правило Борна, проекционные измерения и наблюдаемые. Эволюция в картине Гейзенберга. Смешанные состояния, матрица плотности. Составные системы, тензорное произведение пространств состояний. Перепутанные состояния, редуцированная матрица плотности, разложение Шмидта и очищение. §2. Различимость квантовых состояний Расстояние между классическими распределениями вероятности. Расстояния между квантовыми состояниями. Следовая метрика, фиделити, метрика Бюреса. Соотношения между различными метриками на пространстве состояний. §3. Энтропия фон Неймана. Энтропия фон Неймана для квантовых состояний, количественная оценка чистоты. Квантовая относительная энтропия, её основные свойства. Выпуклость и субаддитивность квантовой энтропии. §4. Квантовые процессы и шумные каналы связи Формализм квантовых процессов, вполне положительные и сохраняющие след отображения. Представление операторной суммой, хи-матрица процесса. Примеры квантовых процессов: канал с X-	32	22	10		32	4 часа Решение задач для закрепления понимания формализма квантовой теории. Эволюция двухуровневой системы, сфера Блоха, белловские состояния и т.п. 4 часа Решение задач, например: на вычисление расстояний в различных метриках, вывод выражения для фиделити через компоненты вектора Блоха для двухуровневой системы. 2 час Решение задач на свойства энтропии фон Неймана. 4 часа Решение задач на преобразование состояний различными каналами. Написание		18

ошибкой и Z-ошибкой, деполяризующий канал, канал затухания амплитуды и фазы (продольная и поперечная релаксация). Представление о квантовой томографии состояний и процессов, информационно-полный набор измерений, методы статистической обработки результатов томографических измерений. §4. Передача классической и квантовой информации по квантовым каналам связи. Задача различения квантовых состояний. Граница Холево. Теорема Шумахера о кодировании в канале без шума. Передача данных через квантовый канал с шумом. Квантовое неравенство обработки данных, граница Синглтона, квантовое неравенство Фано. §5. Количественная теория перепутанности. Преобразования сохраняющие и изменяющие перепутанность, LOCC преобразования. Дистилляция перепутанности, количественные меры перепутанности в двухкомопнентных системах. Перепутанность смешанных состояний, связанная перепутанность. Меры перепутанности в бесконечномерных системах. Проблемы характеризации перепутанности в многокомпонентных системах.						программы для восстановления состояния по результатам томографических измерений. 4 часа. Задачи на методы различения квантовых состояний, unambiguous измерения. 4 часа. Решение задач на количественные меры перепутанности.		
						14 часов Подготовка к промежу-точной аттестации (за-чету).		14
Промежуточная аттестация - зачет	34	24	10		34			34

* Текущий контроль успеваемости в рамках занятий семинарского типа реализуется в форме по рейтинговой системе с учётом результатов проверки домашних заданий, работы в аудитории и результатов выполнения практических компьютерных заданий.

8. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

8.1 Основная и дополнительная литература доступная студентам через Интернет или по запросу лектору.

8.2 Электронные презентации основных тем дисциплины доступные через сайт Центра квантовых технологий: http://quantum.msu.ru/....

9. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Типовые вопросы к зачёту:

1. Квантовая относительная энтропия, её основные свойства
2. Представление процесса операторной суммой, хи-матрица процесса
3. Задача различения квантовых состояний. Граница Холево.
4. Теорема Шумахера о кодировании в канале без шума.

Типовые задачи к экзамену:

1. Покажите, что расстояние между распределениями вероятностей (p,1-p) и (q,1-q) в следовой метрике равно |p-q|
2. Найдите энтропию, связанную с подбрасыванием (а) «честной» монеты, (б) «честной» игральной кости. Что произойдет с энтропией, если монета или кость «нечестные»?
3. Докажите, что двоичная энтропия Ндв(p) принимает максимальное значение при p = 1/2.
4. Пусть |AB>— чистое состояние составной системы, принадлежащей Алисе и Бобу. Покажите, что |AB> является запутанным состоянием тогда и только тогда, когда S(B\A) < 0.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ПОКАЗАТЕЛИ ДОСТИЖЕНИЯ ЗАДАННОГО УРОВНЯ ОСВОЕНИЯ КОМПЕТЕНЦИЙ)

ВЛАДЕТЬ: профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений (В1, СПК-1).

ВЛАДЕТЬ: навыками поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений (В2, СПК-2).

ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений (В3, СПК-3).

УМЕТЬ: анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов (У1, СПК-1).

УМЕТЬ: осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений (У2, СПК-2).

УМЕТЬ: организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования (У3, СПК-3).

ЗНАТЬ: методы анализа и оценки современных научных достижений, а также методы генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений (З1, СПК-1).

ЗНАТЬ: способы критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений (З2, СПК-2).

ЗНАТЬ: методы организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования (З3, СПК-3).

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	**Критерии оценивания результатов обучения**				
	1	**2**	**3**	**4**	**5**

ВЛАДЕТЬ: профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений (В1, СПК-1).	Отсутствие навыков	Фрагментарное применение навыков анализа и синтеза физической информации в области физики квантовых вычислений	В целом успешное, но не систематическое применение навыков анализа и синтеза физической информации в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы применение навыков анализа и синтеза физической информации в области физики квантовых вычислений	Успешное и систематическое применение навыков анализа и синтеза физической информации в области физики квантовых вычислений
ВЛАДЕТЬ: навыками поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений (В2, СПК-2).	Отсутствие навыков	Фрагментарное применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	В целом успешное, но не систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	Успешное и систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений
ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики	Отсутствие навыков	Фрагментарное применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области	В целом успешное, но не систематическое применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских	В целом успешное, но содержащее отдельные пробелы применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых	Успешное и систематическое применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых

квантовых вычислений (В3, СПК-3).		физики квантовых вычислений	задач в области физики квантовых вычислений	вычислений	вычислений
УМЕТЬ: анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов (У1, СПК-1).	Отсутствие умения	Фрагментарное проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешное, но не систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешное, но содержащее отдельные пробелы проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	Успешное и систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов
УМЕТЬ: осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений (У2, СПК-2).	Отсутствие умения	Фрагментарное проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	В целом успешное, но не систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	Успешное и систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений

УМЕТЬ: организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования (У3, СПК-3)	Отсутствие умения	Фрагментарное проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	В целом успешное, но не систематическое проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	В целом успешное, но содержащее отдельные пробелы проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования
ЗНАТЬ: методы анализа и оценки современных научных достижений, а также методы генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений (З1, СПК-1)	Отсутствие знаний	Фрагментарное проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых	В целом успешное, но не систематическое проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики	В целом успешное, но содержащее отдельные пробелы проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений	Успешное и систематическое проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений

		вычислений	квантовых вычислений		
ЗНАТЬ: способы критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений (З2, СПК-2).	Отсутствие знаний	Фрагментарное проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	В целом успешное, но не систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	Успешное и систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений

ЗНАТЬ: методы организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования (З3, СПК-3)	Отсутствие знаний	Фрагментарное проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	В целом успешное, но не систематическое проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	В целом успешное, но содержащее отдельные пробелы проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования

10. Перечень основной и дополнительной учебной литературы

Основная литература

1. M.A. Nielsen, I.L. Chuang Quantum Computation and Quantum Information, 10th anniversary edition, Cambridge University Press, Cambridge, UK, 2010.

Дополнительная литература

1. S. Arora, B. Barak, Computational Complexity: A Modern Approach, Princeton University (http://www.cs.princeton.edu/theory/complexity/)
2. D.A.Lidar, T.A.Brunn, Quantum Error Correction, Cambridge University Press, Cambridge, UK, 2013

11. Перечень ресурсов Интернет необходимых для освоения дисциплины:

- https://quantumexperience.ng.bluemix.net/

12. Методические указания для обучающихся по освоению дисциплины

Для освоения дисциплины необходимо посещение интерактивных занятий (лекций и семинаров) и регулярная самостоятельная работа в течение семестра. Также настоятельно рекомендуется выполнение практических работ на симуляторе/ облачном квантовом компьютере для

получения навыков программирования реального квантового процессора. Для части тем курса имеются электронные презентации, выложенные на сайте Центра.

13. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

При реализации учебной работы в рамках дисциплины «Введение в квантовую информацию» используются средства дистанционного сопровождения учебного процесса в форме сайтов с материалами лекций и семинарских занятий. Курс имеет электронные версии (презентации) лекций. Лекции читаются с использованием современных мультимедийных возможностей и проекционного оборудования.

14. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В соответствии с требованиями п. 5.3. образовательного стандарта МГУ по направлению подготовки «Физика». Любая аудитория, оснащенная проекционным оборудованием с возможностью подключения к ноутбуку, экраном, и учебной доской.