Рабочая программа дисциплины

1. Название дисциплины: Физические генераторы случайных чисел

2. Уровень высшего образования – магистратура

3. Направление подготовки: 03.04.02 Физика (магистратура)

4. Аннотация:

Курс «Физические генераторы случайных чисел» является профильной дисциплиной магистерской программы «Квантовая криптография и квантовая связь». Дисциплина знакомит слушателей с принципами генерации случайных чисел для применений в системах квантовой крипографии и в других вариантах защищенной связи. В курсе рассматриваются фундаментальные принципы генерации случайных чисел, математический аппарат, требуемый для обработки сырых данных и формирования выходной случайной последовательности, а также примеры практического применения этих принципов в конечных устройствах.

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 часов составляет контактная работа обучающегося с преподавателем (18 часов занятия лекционного типа, 16 часов занятия семинарского типа, 2 часа коллоквиумов), 36 часов 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 дисциплин «Квантовая механика», «Основы квантовой оптики», а также математических дисциплин «Линейная алгебра» и «Теория вероятности и стохастические процессы». Желательно также предварительно освоить дисциплину «Криптография и элементы теории информации».

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. Введение Введение в теорию генерации случайных чисел. Необходимость их использования для криптографических применений, численного моделирования и моделирования случайных процессов.		1			1	1 час Знакомство с обзорами по генерации случайных чисел.		1

2. Регистры сдвига и программные генераторы случайных чисел. §1. Простейшие примеры регистров сдвига. Случайные последовательности PRBS7, PRBS9. Полиномиальное представление генераторов. §2. Примеры использования регистров сдвига для измерения вероятности ошибок в цифровых каналах связи. Тестеры доли битовых ошибок (BERT). §3. Современные псевдослучайные генераторы. Детерминистические последовательности с большим периодом. Системные генераторы случайных чисел /dev/random, /dev/urandom.		3	2		5	1 час Вычисление периода для конкретного регистра сдвига. 2 час Самостоятельное изучение графических методов тестирования на случайность применительно к регистрам сдвига. 4 часа Повторение лекционного материала по теме «Регистры сдвига и программные генераторы случайных чисел».		7
3. Физические принципы генерации случайных чисел §4. Источники случайности в рамках классической физики. Доска Гальтона. Предсказуемость любой классической системы. Недостатки такого рода источников. §5. Квантовые принципы генерации случайных чисел. Неравенства Белла и теория скрытых переменных. Нарушение принципа локального реализма.		2	2		4	2 часа Самостоятельное изучение обзоров по неравенствам Белла.		2
4. Неидеальность физических источников случайных чисел. Методы экстракции.		4	2	2 часа Коллоквиум по	8	8 часов Подготовка к коллокви-		8

§6. Методы непосредственной минимизации неидельности источника с помощью цепей обратной связи. §7. Детерминистическая экстракция случайных чисел. Метод Фон Неймана. Достоинства и недостатки, пример реализации таких экстракторов. Метод Элиаса. §8. Энтропия источника случайности. Практическая значимость и методы ее оценки. §9. Случайные экстракторы. Случайные матрицы Тёплица. Сильные и слабые экстракторы. Использование выхода генератора случайных чисел для реинициализации случайного экстрактора. Достоинства и недостатки случайных экстракторов.				пройденным темам		уму		
5. Основные реализации квантовых генераторов случайных чисел. §10. Системы с дискретной однофотонной регистрацией. Подсчет числа событий, измерение временных интервалов между событиями. Системы со светоделителями. §11. Системы с непрерывным детектированием. Измерение фазовых шумов лазера.		3	3		6	2 часа Самостоятельное изучение литературы по отклонениям коммерчески доступных генераторов случайных чисел от идеальных.		2
6. Тесты на случайность. §12. Программный пакет NIST. Разбор основных типов тестов. Вычисление распределения вероятностей для простейших вариантов тестов. Тесты Diehard. Примеры детерминистических последовательностей, проходящих тесты на случайность.		4	4		8	2 часа Вычисление распределения вероятностей для одного из тестов пакета NIST.		2

Промежуточная аттестация - зачет			4		4	14 часов Подготовка к промежуточной аттестации (зачету).		14
Итого		18	16	2	36			36

* Текущий контроль успеваемости в рамках занятий семинарского типа реализуется в форме обсуждения.

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.

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

Типовые контрольные вопросы и темы для обсуждения:

1. Периоды псевдослучайных генераторов на регистрах сдвига.
2. Принципы детерминистической экстракции случайных последовательностей.
3. Энтропия источника случайности.
4. Различия между квантовой случайностью и случайностью в классической физике.
5. Пример квантового генератора случайных чисел с дискретным однофотонным детектором.
6. Оцифровка аналогового источника шума. Время декогеренции.
7. Частотный тест на случайность.
8. Спектральный тест на случайность.
9. Тест на сжатие случайной последовательности.
10. Тест с вычислением аппроксимированной энтропии.

Типовые вопросы к зачету:

1. Регистры сдвига PRBS7, PRBS9. Вычисление периода генерируемой последовательности.
2. Принципы работы тестеров доли битовых ошибок на регистрах сдвига.
3. Современные системные генераторы случайных чисел. Отличие от традиционных псевдослучайных генераторов.
4. Классическая случайность на примере доски Гальтона.
5. Квантовая случайность. Нарушение принципа локального реализма.

6. Неравенства Белла и теория скрытых переменных.
7. Пример физического генератора случайных чисел без экстрактора. Автоподстройка.
8. Детерминистическая экстракция случайных чисел. Метод Фон Неймана.
9. Экстракция случайных чисел с помощью метода Элиаса.
10. Энтропия источника случайности. Методы ее оценки.
11. Расчет энтропии для несимметричной монетки. Эффективность экстракции. Примеры.
12. Случайные экстракторы на примере матриц Тёплица.
13. Принципы действия тестов на случайность. Конкретный пример с вычислением вероятностей.
14. Частотный тест на случайность.
15. Спектральный тест на случайность.
16. Тест на сжатие случайной последовательности.
17. Тест с вычислением аппроксимированной энтропии.
18. Достаточно ли прохождения тестов на случайность для гарантии хорошего качества источника? Примеры.

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 инфор-мации 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,	Отсутствие навыков	Фрагментарное применение навыков	В целом успешное, но не систематическое	В целом успешное, но содержащее отдельные	Успешное и систематическое применение навыков

критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений (В2, СПК-2).		поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	пробелы применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	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 квантовых вычислений (В3, СПК-3).	Отсутствие навыков	Фрагментарное применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений	В целом успешное, но не систематическое применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений	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 вычислений	Успешное и систематическое применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых 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. Herrero-Collantes, J. C. Garcia-Escartin "Quantum Random Number Generators", Reviews of Modern Physics 89, 015004 (2017) (https://arxiv.org/abs/1604.03304).
2. T. Kennedy "Monte Carlo Methods - a special topics course" (https://www.math.arizona.edu/~tgk/mc/book.pdf)
3. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" NIST (2010) (https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic).

Дополнительная литература

4. K. S. Kravtsov, I. V. Radchenko, S. P. Kulik, and S. N. Molotkov, “Minimalist design of a robust real-time quantum random number generator,” J. Opt. Soc. Am. B, vol. 32, no. 8, pp. 1743–1747, 2015.
5. L. Trevisan, “Extractors and pseudorandom generators,” Journal of the ACM 48, 860–879 (2001).

6. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, “Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction,” Phys. Rev. A 87, 062327 (2013).
7. W. Mauerer, C. Portmann, and V. B. Scholz, “A modular framework for randomness extraction based on Trevisan’s construction,” (2012). arXiv:1212.0520 [cs.IT].
8. P. Elias, “The efficient construction of an unbiased random sequence,” Ann. Math. Statist. 43, 865–870 (1972).
9. Y. Peres, “Iterating von Neumann’s procedure for extracting random bits,” Ann. Statistics 20, 590–597 (1992).
10. A. Juels, M. Jakobsson, E. Shriver, and B. K. Hillyer, “How to turn loaded dice into fair coins,” IEEE Trans. Inform. Theory 46, 911–921 (2000).

11. Перечень ресурсов Интернет необходимых для освоения дисциплины:

- https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic

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.

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

- средства дистанционного сопровождения учебного процесса в форме сайта с избранными материалами лекций и семинарских занятий.
- 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.