Рабочая программа дисциплины

1. Название дисциплины: Протоколы квантовой криптографии от теории к практике

2. Уровень высшего образования – магистратура

3. Направление подготовки: 03.04.02 Физика (магистратура)

4. Аннотация:

Курс «**Квантовая криптография**» является профильной дисциплиной магистерской программы «Квантовая криптография и квантовая связь». Дисциплина обеспечивает подготовку студентов в области методов фундаментальных знаний в новой области современных исследований -- квантовой криптографии. Цели также включают в себя:

1) Освоение математического аппарата, используемого для задач квантовой криптографии.

2) Освоение принципов работы базовых квантовых криптографических протоколов распределения ключей.

3) Освоение принципов работы волоконно-оптических систем квантового распределения ключей, а также систем квантовой криптографии, работающих через открытое пространство.

4) Получение навыков разработки и доказательства криптографической стойкости систем квантовой криптографии.

5) Подготовка студентов к чтению современной научной литературы в данной области.

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

5. 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 квантовой электроники и квантовых технологий.

СПК-2 Способность к поиску, критическому анализу, обобщению и систематизации научной информации в области квантовой электроники и квантовых технологий.

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

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВЕНЬ 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 базовые протоколы кантового распределения ключей. Основные фундаментальные принципы работы и устройство современных систем квантового распределения криптографических ключей, понятийный и математический аппарат, используемый при доказательстве стойкости систем квантовой криптографии, как в оптоволоконном варианте, так и работающих через открытое пространство. Различные виды атак на такие системы, а также методов противодействия им. Знать и понимать принципиальные отличия и новые возможности, по сравнению с классическими методами распределения ключей.

УМЕТЬ: Применять полученные знания при решении и постановке типовых задач в области квантовой криптографии. Анализировать криптографическую стойкость таких систем по отношению к различным атакам на них. Работать с современными поисковыми системами и базами данных с научной литературой.

ВЛАДЕТЬ: навыками анализа таких систем и навыками решения теоретических практических задач в области квантовой криптографии. Для освоения дисциплины необходимы знания и умения, приобретаемые в рамках дисциплин общей физики «Оптика», «Математический анализ», «Линейная алгебра».

6. 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**
Методы практической чистки первичных ключей и методы сжатия (хэширования – усиления секретности) ключей в квантовой криптографии. Методы коррекции ошибок основанные на классических кодах корректирующих ошибки. Итерационные адаптивные процедуры исправления ошибок.		4			**4**	4		**4**
Анализ стойкости реализаций систем квантовой криптографии с не идеальными источниками квантовых состояний, детекторами и квантовым каналом связи с потерями. Атака с расщеплением по числу фотонов. Атака с подменой фазы в системах с фазовым кодированием. Атака с ослеплением фотодетекторов.		4			**4**	4		**46**
Протоколы устойчивые по отношению к атаке с ослеплением фотодетекторов. Побочные каналы утечки информации в системах квантовой криптографии, фундаментальная квантово-механическая верхняя граница на утечку информации по побочным каналам.		2			**2**	2		**2**

Основы математического аппарата для анализа стойкости систем квантовой криптографии с конечными длинами передаваемых последовательностей. Критерий составной секретности ключей, основанный на следовом расстоянии.		2			**2**	2		**2**
Основные свойства квантовых энтропий Реньи (min и max энтропий). Сглаженные min и max энтропии, цепочечные правила, изменение min и max энтропий при действии супероператора, свойства min и max энтропии для составных квантовых систем.		2			**2**	2		**2**
Teopems de Finetti классический и квантовые случаи. Min и max энтропий для тензорного произведения матриц плотности. Симметричные состояния. Min и max энтропий для симметричных состояний. Необходимые неравенства для различных расстояний между квантовыми состояниями.		6			**6**	6		**6**
Коррекция ошибок с минимальной утечкой информации при помощи универсальных хэш-функций второго порядка.		4			**4**	2		**2**
Квантовое усиление секретности. Квантовая теорема усиления секретности – теорема об остатке хэширования. Примеры доказательств секретности BB84 и фазово-временной квантовой криптографии с использованием аппарата квантовых min и max энтропий (асимптотический предел).		2			**2**	2		**2**

Энтропийные соотношения неопределенностей в квантовой криптографии. Связь с min и max энтропиями.		2			**2**	2		**2**
Анализ стойкости квантового протокола распределения ключей BB84 с конечными передаваемыми последовательностями (доказательство с использованием энтропийных соотношений неопределенности).		2			**2**	2		**2**
Доказательства стойкости фазово-временной и релятивистской квантовой криптографии для открытого пространства с конечными длинами последовательностей с использованием аппарата квантовых min и max энтропий.		2			**2**	2		**2**
Промежуточная аттестация - зачет			4		**4**	4 Подготовка к промежуточной аттестации (зачету).		**4**
Итого		32	4	2	**36**			**36**

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

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

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

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

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ПОКАЗАТЕЛИ ДОСТИЖЕНИЯ ЗАДАННОГО УРОВНЯ ОСВОЕНИЯ КОМПЕТЕНЦИЙ)

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

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

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

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

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

УМЕТЬ: организовывать и планировать исследования, ставить конкретные задачи научных исследований в области квантовых оптических технологий, 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 квантовых оптических технологий (З1, СПК-1).

ЗНАТЬ: способы критического анализа и систематизации научной информации при решении исследова¬тельских задач в области квантовых оптических технологий (З2, СПК-2).

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

Планируемые	**Критерии оценивания результатов обучения**

результаты обучения **(показатели достижения заданного уровня освоения компетенций)**	**1**	**2**	**3**	**4**	**5**
ВЛАДЕТЬ: профессиональными знаниями для анализа и синтеза физической информации в области квантовой электроники и квантовых технологий. (В1, СПК-1).	Отсутствие навыков	Фрагментарное применение навыков анализа и синтеза физической информации в области квантовой электроники и квантовых технологий	В целом успешное, но не систематическое применение навыков анализа и синтеза физической информации в области квантовой электроники и квантовых технологий	В целом успешное, но содержащее отдельные пробелы применение навыков анализа и синтеза физической информации в области квантовой электроники и квантовых технологий	Успешное и систематическое применение навыков анализа и синтеза физической информации в области квантовой электроники и квантовых технологий
ВЛАДЕТЬ: навыками поиска, критического анализа, обобщения и систематизации научной информации в области квантовой электроники и квантовых технологий (В2, СПК-2).	Отсутствие навыков	Фрагментарное применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области квантовой электроники и квантовых технологий	В целом успешное, но не систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области квантовой электроники и квантовых технологий	В целом успешное, но содержащее отдельные пробелы применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области квантовой электроники и квантовых технологий	Успешное и систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области квантовой электроники и квантовых технологий
ВЛАДЕТЬ: навыками анализа	Отсутствие навыков	Фрагментарное применение навыков	В целом успешное, но не систематическое	В целом успешное, но содержащее отдельные	Успешное и систематическое применение

методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области квантовой электроники и квантовых технологий (В3, СПК-3).		анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области квантовой электроники и квантовых технологий	применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в квантовой электроники и квантовых технологий	пробелы применение навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области квантовой электроники и квантовых технологий	навыков анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области квантовой электроники и квантовых технологий
УМЕТЬ: анализировать альтернативные варианты решения исследовательских задач в области квантовой электроники и квантовых технологий и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов (У1, СПК-1).	Отсутствие умения	Фрагментарное проявление умения анализировать альтернативные варианты решения исследовательских задач в области квантовой электроники и квантовых технологий и оценивать потенциальные выигрыши/ проигрыши реализации этих вариантов	В целом успешное, но не систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области квантовой электроники и квантовых технологий 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 квантовой электроники и квантовых технологий и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	Успешное и систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области квантовой электроники и квантовых технологий и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов

УМЕТЬ: осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области квантовой электроники и квантовых технологий (У2, СПК-2).	Отсутствие умения	Фрагментарное проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области квантовой электроники и квантовых технологий	В целом успешное, но не систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области квантовой электроники и квантовых технологий	В целом успешное, но содержащее отдельные пробелы проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области квантовой электроники и квантовых технологий	Успешное и систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области квантовой электроники и квантовых технологий
УМЕТЬ: организовывать и планировать исследования, ставить конкретные задачи научных исследований в области квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, и решать их с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление организовывать и планировать исследования, ставить конкретные задачи научных исследований в области квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий (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 квантовой электроники и квантовых технологий	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 квантовой электроники и квантовых технологий	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 квантовой электроники и квантовых технологий	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 квантовой электроники и квантовых технологий
ЗНАТЬ: способы критического анализа и систематизации научной информации при решении исследовательских задач в области квантовой электроники и квантовых технологий (З2, СПК-2).	Отсутствие знаний	Фрагментарное проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области квантовой электроники и квантовых технологий	В целом успешное, но не систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области квантовой электроники и квантовых технологий	В целом успешное, но содержащее отдельные пробелы проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области квантовой электроники и квантовых технологий	Успешное и систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области квантовой электроники и квантовых технологий

ЗНАТЬ: методы организации и планирования исследований в области квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, 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 квантовой электроники и квантовых технологий, включая способы решения задач с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление знаний методов организации и планирования исследований в области квантовой электроники и квантовых технологий, включая способы решения задач с помощью современной аппаратуры и оборудования

9. Перечень основной и дополнительной учебной литературы

Основная литература:

1. А.С.Холево. Квантовые системы, каналы, информация, Москва. МЦМО, сс.327 (2010); S. Holevo, Introduction to Quantum Information Theory, (MTNMO, Moscow, 2002) [in Russian]; Usp. Mat. Nauk, 53, 193 (1998); А.С.Холево, Введение в квантовую теорию информации, серия Современная математическая физика, вып.5}, МЦНМО, Москва, 2002
2. М.Нильсен, И.Чанг, Квантовые вычисления и информация, изд. Мир, Москва, (2006).
3. Дж. Прескилл, Квантовая информация и квантовые вычисления, том 1, изд. R&C Dynamics, Ижевск, (2008).
4. C.E.Shannon, Mathematical Theory of Communication, Bell Syst. Tech. Jour., 27, 397; 27, 623 (1948).
5. Р.Галлагер, Теория информации и надежная связь, (Советское радио, 1974);
6. R. G. Gallager, Information Theory and Reliable Communication, (Wiley, New York, 1968)

Дополнительная литература:

1. W.K.Wootters, W.H.Zurek, A single quantum cannot be cloned, Nature, {299, 802 (1982).

2. C.H.Bennett, G.Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 175 (1984).
3. C.H.Bennett, Phys. Rev. Lett., 68, 3121 (1992).
4. R.Renner, Security of Quantum Key Distribution, PhD Thesis, ETH Z\"urich, Dec. 2005. arXiv/quant-ph: 0512258.
5. V.Scarani, H.Bechmann-Pasquinucci, N.J.Cerf, M.Dusek, N.Lutkenhaus,
6. M.Peev, Rev. Mod. Phys., 81, 1301 (2009).
7. D.Mayers, Journal ACM, 48 351 (2001).
8. H.-K.Lo, H.F.Chau, Science, 283 2050 (1999).
9. P.Shor, J.Preskill, Phys. Rev. Lett., 85 441 (2000).
10. M.Koashi, J. Phys. Conf. Ser., 36, 98 (2006).
11. M.Tomamichel. R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.
12. M.Tomamichel, C.Ci Wen Lim, N.Gisin, R.Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv/quant-ph: 11034130.
13. С.П.Кулик, А.П.Маккавеев, С.Н.Молотков, Письма в ЖЭТФ. 85, 354 (2007).
14. С.Н.Молотков, ЖЭТФ. 133, 5 (2008).
15. Д.А.Кронберг, С.Н.Молотков, ЖЭТФ, 136, 650 (2009); ЖЭТФ, 138, 33 (2010).
16. H.P.Robertson, Phys. Rev., 34, 163 (1929).
17. D.Deutsch, Phys. Rev. Lett., 50, 631 (1983).
18. K.Kraus, Phys. Rev., D 35, 3070 (1987).
19. H.Maassen, J.B.M.Uffink, Phys. Rev. Lett., {\bf 60}, 1103 (1988).
20. J.M.Renes, J.-C. Boileau, Phys. Rev. Lett., 103, 020402-1 (2009).
21. M.Berta, M.Chritlandl, R.Colbeck, J.M.Renes, R.Renner, The Uncertainty Principle in the Presence of Quantum Memory, arXiv/quant-ph: 0909.0950.
22. M.Cover J.A.Thomas. Elements of Information Theory. Wiley, (1991).
23. M.Berta, M.Christandl, R.Colbeck, J.M.Renes, R.Renner, Nature Physics, 6, 659 (2010).
24. M.Tomamichel, R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.
25. J.M.Renes, R.Renner, One-Shot Classical Data Compression withQuantum Side Information and the Distillation of Common Randomness or Secret Keys, arXiv/quant-ph: 10080452.
26. J.L.Carter, M.N.Wegman Universal Classes of Hash Functions, J. Comp. Syst. Sci., 18, (1979) 143.
27. M.N.Wegman, J.L.Carter, New Hash Functions and Their Use Authentication and Set Euqality, J. Comp. Syst. Sci., 22, 265 (1991).
28. C.H.Bennett, G.Brassard, C.Crepeau, U.M.Maurer, Generalized Privacy Amplication, IEEE Trans. on Inf. Theory, 41 (1995) 1915.
29. M.Tomamichel, C.Schaffner, A.Smith, R.Renner, Leftover Hashing Against Quantum Side Information, arXiv/quant-ph: 10022436.
30. D.R.Stinson, On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes, ECCC TR95-052, Electronic Colloquium on Computational Complexity - Reports Series (1995).
31. W.Hoeffding, Probability Inequalities for Sums of Bounded Random Variables, J. Amer. Statistical Assoc., 58 (1963) 13.

32. R. J. Serfling, Probability Inequalities for the Sum in Sampling without Replacement ,Ann. Stat., 2 (1974) 39.
33. L.Lydersen, C.Wiechers, C.Wittmann, D.Elser, J.Skaar, V.Makarov,
34. Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics, 4, 686 (2010).
35. С.Н.Молот ков, “Энтропийные соотношения неопределенностей и стойкость фазово-временной квантовой криптографии при конечных длинах передаваемых последовательностей” Журнал экспериментальной и теоретической физики, т. 142 (2012) 1-19.
36. С.Н.Молотков, “О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах”.Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 374.
37. С.П.Кулик, С.Н.Молотков, И.В.Радченко, “О квантовом распределении ключей на композитных фотонах -- поляризационных кутритах.” Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 367.
38. С.Н.Молотоков, “О геометрически однородных когерентных состояниях в квантовой криптографии”, Письма в журнал экспериментальной и теоретической физики, т. 95 (2012) 361.
39. С.Н.Молотков, “Об уязвимости базовых протоколов квантового распределения ключей и о трех протоколах, устойчивых к атаке с “ослеплением” лавинных детекторов”, Журнал экспериментальной и теоретической физики, т. 141 (2012) 812-831.
40. С.Н.Молотков,“О решении проблемы обеспечения стойкости квантовой криптографии для канала связи со сколь угодно большой длиной”, Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 830.
41. С.Н.Молотков,“Квантовое распределение ключей без передачи квантового состояния как целого через канал связи”, Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 389.
42. С.Н.Молотков, “Релятивистская квантовая криптография для открытого пространства без синхронизации часов на передающей и приемной стороне”, Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 504.
43. С.Н.Молотков, “Энтропийные соотношения неопределенностей и предельно допустимая критическая ошибка в квантовой криптографии”. Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 900.
44. Молотков, “Квантовое распределение ключей с эталонным квантовым состоянием”, Журнал экспериментальной и теоретической физики, т. 140 (2011) 857.
45. С.Н.Молотков, Релятивистская квантовая криптография, Журнал экспериментальной и теоретической физики, т. 139 (2011) 139.
46. Д.А.Кронберг, С.Н.Молотков, Усиление стойкости фазово-временной квантовой криптографии блочным исправлением ошибок,, Письма в ЖЭТФ, т.92, (2010) 539.
47. Д.А.Кронберг, С.Н.Молотков, Квантовая схема для оптимального подслушивания фазово-временной квантовой криптографии ,ЖЭТФ, т.138 (2010) 33.

10. Перечень ресурсов Интернет необходимых для освоения дисциплины:

1. Основной Интернет-ресурс по квантовой информатике и квантовой криптографии: международный архив электронных препринтов Корнельского университета: xxx.lanl.gov\quant-ph

2. http://www.aps.org – журналы Американского физического общества,
3. jetpletters.ac.ru, jetp.ac.ru – журналы Российской академии наук.

11. Методические указания для обучающихся по освоению дисциплины

Для освоения дисциплины необходимо посещение интерактивных занятий и регулярная самостоятельная работа в течение семестра.

12. 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 используются средства дистанционного сопровождения учебного процесса. Лекции читаются с использованием современных мультимедийных возможностей и проекционного оборудования.

13. 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.