Рабочая программа дисциплины

1. Название дисциплины: Постквантовая криптография: методы криптографической защиты информации в эпоху развития квантовых компьютеров

2. Уровень высшего образования – магистратура

3. Направление подготовки: 03.04.02 Физика (магистратура)

4. Аннотация:

Курс «Постквантовая криптография: методы криптографической защиты информации в эпоху развития квантовых компьютеров» является профильной дисциплиной магистерской программы «Квантовая криптография и квантовая связь». Дисциплина призвана дать представление слушателям об основных задачах, решаемых с использованием криптографии, актуальных методах синтеза и анализа криптографических механизмов, среди которых алгоритмы блочного шифрования, функции хэширования, схемы подписи и протоколы выработки общего ключа. Представлены перспективные методы синтеза криптографических механизмов, стойких к атакам с использованием квантового компьютера (постквантовых криптографических механизмов), среди которых теория решеток, коды исправляющие ошибки, многочлены от многих переменных, итеративное использование функций хэширования. Знание основных принципов лежащих в основе синтеза и анализа как классических, так и постквантовых криптографических механизмов является ключевым элементом при разработке квантовых вычислителей предназначенных для решения задач криптографического анализа.

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.

ИК-3, ИК-4, ПК-2, ПК-3, ОНК-5, ОНК-6, СК-1

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 в криптографию. §1. Основные задачи криптографии. §2. Принципы создания средств криптографической защиты информации (СКЗИ).		2	2		4	2 часа Термины, определения и задачи криптографии. Понятие теоретической и практической стойкости. 2 часа Изучение типовых узлов и блоков современных СКЗИ, принципы создания функционально		4

						законченных криптографических атак.		
2. Основные синтезные принципы криптографических механизмов. §3. Блочные шифры. Методы синтеза раундовых преобразований блочных шифров. Сети Фейстеля, SP-сети, XSL схемы. §4. Режимы работы блочных шифров, их криптографические и эксплуатационно-технические свойства. §5. Бесключевые и ключевые функции хэширования. Итеративные способы построения хэш-функций. §6. Криптография с открытым ключом. Связь асимметричных систем с математическими проблемами (факторизация, дискретное логарифмирование). Схемы цифровой подписи RSA, Эль-Гамаля, Шнорра. §7. Протоколы открытого распределения ключей.		4	4		8	2 часа Изучение общих принципов функционирования блочных шифров DES, AES, «Магма», Кузнечик и режимов работы. 1 часа Изучение общих принципов функционирования функций хэширования семейств SHA, «Стрибог». 1 часа Изучение общих принципов функционирования функций схем подписи RSA, DSA, ГОСТ Р 34.10-2012		4

3. Общие методы анализа криптографических механизмов §8. Методы анализа блочных шифров. S-блоки и их свойства. §9. Криптографический анализ режимов работы шифра. Режимы работы блочных шифров их криптографические и эксплуатационно-технические свойства. §10. Общие методы анализа функции хэширования. §11. Анализ схемы цифровой подписи и протоколов открытого распределения ключей. Методы анализа, основанные на поиске коллизий для используемых функций хэшировани и на решении базовых теоретико-сложностных задач.		4	2	2 часа Коллоквиум по пройденным темам	8	1 часа Изучение общих принципов дифференциального и линейного методов криптографического анализа 1 часа Изучение общих принципов методов анализа функций хэширования, основанных на «парадоксе дней рождений» 1 часа Изучение общих принципов применения методов дискретного логарифмирования при анализе схем цифровой подписи 5 часов Подготовка к коллокви-уму		8
4. Подходы к использованию квантового компьютера при построении методов анализа		4	2		6	3 часа Знакомство с оригинальными статьями		3

криптографических механизмов §12. Особенности применяя квантового компьютера при анализе критпографических механизмов §13. Алгоритм Гровера. Применение алгоритма при анализе блочных шифров и функций хэширования. §14. Алгоритм Саймона. Применение протокола при анализе функций хэширования. §15. Алгоритм Шора. Применение алгоритма и его модификаций при анализе схем цифровой подписи.						по использованию квантового компьютера при проведении криптографического анализа		
5**. Подходы к построению постквантовых криптографических механизмов** §10. О возможности использования методов классической криптографии при построении посквантовых криптографических механизмов. §9. Методы, основанные на использовании теории решеток. §10. Методы, основанные на использовании многочленов от многих переменных. §11. Методы, основанные на использовании теории кодов. §12. Методы, основанные на итеративном использовании функций хэширования.		4	2		6	3 часа Знакомство с материалами конкурса NIST-PQ		3
Промежуточная аттестация - зачет			4		4	15 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. Задачи криптографии. Понятие стойкости
2. Наиболее распространенные алгоритмы блочного шифрования
3. Наиболее распространенные функции хэширования
4. Наиболее распространенные схемы цифровой подписи и протоколы открытого распределения ключей
5. Принципы создания функционально законченных СКЗИ
6. Метод дифференциального анализа блочных шифров
7. Метод линейного анализа блочных шифров
8. Использование «парадокса дней рождений» при анализе функций хэширования
9. Использование методов дискретного логарифмирования и факторизации при анализе схем подписи и протоколов открытого распределения ключей
10. Алгоритм Гровера
11. Алгоритм Шора
12. Алгоритм Саймона
13. Подходы к использованию квантового компьютера при анализе критпографических механизмов
14. Методы синтеза криптографических механизмов, основанные на теории решеток
15. Методы синтеза криптографических механизмов, основанные на использовании многочленов от многих переменных
16. Методы синтеза криптографических механизмов, основанные на кодах, исправляющих ошибки
17. Методы синтеза криптографических механизмов, основанные на итеративном применении функций хэширования.

Типовые вопросы к зачету:

1. Основные задачи решаемые с использованием криптографических методов
2. Алгоритмы блочного шифрования DES и «Магма»
3. Алгоритмы блочного шифрования AES и «Кузнечик»
4. Функции хэширования семейств SHA «Стрибог»
5. Схемы цифровой подписи RSA, (EC)DSA и ГОСТ Р 34.10-2012
6. Протокол открытого распределения ключей DH и его модификации

7. Принципы создания функционально законченных СКЗИ
8. Применение методов дифференциально анализа при исследовании блочных шифров
9. Применение методов линейного анализа при исследовании блочных шифров
10. Применение «парадокса дней рождений» при анализе функций хэширования
11. Применение методов дискретного логарифмирования и факторизации при анализе схем подписи
12. Применение методов дискретного логарифмирования при анализе протоколов открытого распределения ключей
13. Применение алгоритма Гровера при анализе блочных шифров и функций хэширования
14. Применение алгоритма Шора при анализе схем цифровой подписи и протоколов открытого распределения ключей
15. Применение алгоритма Саймона при анализе функций хэширования
16. Особенности использования методов классической криптографии при синтезе поствквантовых криптографических механизмов
17. Примеры криптографических механизмов, основанных на теории решеток
18. Примеры криптографических механизмов, основанных на использовании многочленов от многих переменных
19. Примеры криптографических механизмов, основанных на кодах, исправляющих ошибки
20. Примеры криптографических механизмов, основанных на итеративном применении функций хэширования.

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,	Отсутствие навыков	Фрагментарное применение навыков поиска, критического	В целом успешное, но не систематическое применение навыков	В целом успешное, но содержащее отдельные пробелы применение навыков	Успешное и систематическое применение навыков поиска, критического анализа,

обобщения и систематизации научной информации в области физики квантовых вычислений (В2, СПК-2).		анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	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	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 вычислений	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 квантовых вычислений	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
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. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации: учебник для академического бакалавриата. – М.: Издательство Юрайт, 2016. - 473 с.
2. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. – М.: Издательство Юрайт, 2017. - 349 с.
3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2005 г.
4. Логачев О.А., Сальников А.А., Ященко В.В.: Булевы функции в теории кодирования и криптологии – М.: МЦНМО, 2004.
5. Фомичев В.М., Криптографические методы защиты информации: учебник для академического бакалавриата в 2 ч. М.: Юрайт, 2017.
6. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г.
7. Кайе Ф., Лафламм Р., М. Введение в квантовые вычисления. Москва-Ижевск: РХД, 2009.
8. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. М.,: МЦНМО, ЧеРо, 1999.
9. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006.
10. Садовничий В. А. (ред.). Квантовые вычисления: за и против. Ижевск: РХД, 1999.
11. Садовничий В. А. (ред.). Квантовый компьютер и квантовые вычисления. Ижевск: РХД, 1999.

12. Глухов М.М., Круглов И.А., Пичкур А.В., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. СПб.: Лань, 2011.
13. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона. Дискретная математика, т. 4(3), 57-63, 1992.
14. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера. Дискретная математика, т. 6(2), 3-20, 1994.
15. Grover L.K. A fast quantum mechanical algorithm for database search. Proc. 28th Annual ACM Symposium on the Theory of Computation, 1996.
16. Grover L.K., Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Lett., 79, pp. 325-328. 1997.
17. NISTIR. Report on Post-Quantum Cryptography. NISTIR 8105. Draft, February 2016.
18. Hüttenhain J., Wallenborn L. Topics in Post-Quantum Cryptography. Lattice-Based Methods. 2011.
19. Bansarkhani R. E. LARA - A Design Concept for Lattice-based Encryption. ePrint report 2017/049.
20. J.-P. Aumasson, G. Endignoux. Improving stateless hash-based signatures. Cryptology ePrint Archive, Report 2017/933, 2017, https://eprint.iacr.org/2017/933
21. J. Buchmann, E. Dahmen, M. Schneider. Merkle tree traversal revisited. In: J. Buchmann, J. Ding (eds.). Post-Quantum Cryptography, vol. 5299 of Lecture Notes in Computer Science, pp. 63-78. Springer Berlin Heidelberg, 2008.
22. A.Hülsing, C. Busold, J. Buchmann. Forward secure signatures on smart cards. In Selected Areas in Cryptography, vol. 7707 of Lecture Notes in Computer Science, pp. 66-80. Springer, 2012.
23. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 44,114–116, Jan. 1978.

Дополнительная литература

1. Бабаш А.В., Шанкин Г.П. Криптография. Под редакцией В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-Р, 2002. – 512 с.
2. Stamp M., Low R.M. Applied cryptanalysis. Breaking ciphers in the real world. Wiley, 2007.
3. Vaudenay S. A classical introduction to cryptography: Applications for communication security, Springer-Verlag, 2006.
4. Baigneres T., Junod P., Li Y., Monnerat J., Vadenau S. A classical introduction to cryptography. Exercise book. Springer-Verlag, 2006.
5. Biham E., Biham O., Biron D., Grassl M., Lidar D. Grover's quantum search algorithm for an arbitrary initial amplitude distribution. Physical Review A, 60(4):2742, 1999. arXiv:quant- ph/9807027,
6. Bravyi S., Harrow A., Hassidim A. Quantum algorithms for testing properties of distributions. IEEE Transactions on Information Theory 57(6):3971-3981, 2011. arXiv:0907.3920.
7. Ekerå M. Modifying Shor’s algorithm to compute short discrete logarithms. eprint.iacr.org/2016/1128
8. Harrow A. W., Hassidim A., Lloyd S. Quantum algorithm for solving linear systems of equations. Physical Review Letters 15(103):150502, 2009. arXiv:0811.3171.
9. Proos J., Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information and Computation, Vol. 3, No. 4, pg.

317-344, 2003. arXiv:quant-ph/0301141.
10. Jordan S. Quantum Algorithm Zoo, http://math.nist.gov/quantum/zoo
11. Anand M.V., Targhi E.E., Tabia G.N., Unruh D. Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation. Cryptology ePrint Archive, Report 2016/197.
12. Lu C.Y. et al.: Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits, Physical Review Letters 99 (25): 250504, arXiv:0705.1684 (2007).
13. IEEE Std 1363.1-2008. Public key cryptographic techniques based on hard problems over lattices.
14. Ajtai M. Generating hard instances of lattice problems. Quaderni di Matematica, 13:1–32, 2004. Preliminary version in STOC 1996.
15. Guneysu T., Lyubashevsky V., Poppelman T. Practical lattice-based cryptography: A signature scheme for embedded systems. CHES 2012, pp/513-547, 2012.
16. Regev O. Learning with Errors Problem. 2010.
17. J. Katz. Analysis of a proposed hash-based signature standard, rev. 4, www.cs.umd.edu/~jkatz/papers/HashBasedSigs.pdf. 2016.
18. NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standartization process, 2016, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
19. Daniels T., Smith-Tone D. Differential Properties of the HFE Cryptosystem. PQC 2014, LNCS 8772, pages 59-75. eprint.iacr.org/2014/398.
20. Porras J., Baena J., Ding J. ZHFE, a New Multivariate Public Key Encryption Scheme. PQC 2014, LNCS 8772, pages 229-245. eprint.iacr.org/2014/387
21. Vates J., Smith-Tone D. Key Recovery Attack for All Parameters of HFE-. PQC 2017, LNCS 10346, pages 272-288.
22. Asaar M. R., Salmasizadeh M., Aref M. R. A Provably Secure Codebased Concurrent Signature Scheme. Cryptology ePrint Archive, Report 2016/449.

11. Перечень ресурсов Интернет необходимых для освоения дисциплины:

- https://arxiv.org/
- http://www.eprint.iacr.org,
- http://www.mathnet.ru.

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.