МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»

«Утверждаю»

Декан факультета ВМК МГУ
имени М.В. Ломоносова

академик _____ И.А. Соколов

«___»_____ 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Математические методы квантовой криптографии»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки – 10.06.01 «Информационная безопасность»

Направленность (профиль) – «Методы и системы защиты информации, информационная безопасность» (05.13.19)

2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Математические методы квантовой криптографии

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 10.06.01 «Информационная безопасность». Направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (05.13.19).

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к специальным дисциплинам вариативной части образовательной программы и является обязательной для освоения в 1-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (СПК-2)	З1(СПК-2) ЗНАТЬ Средства обеспечения информационной безопасности. У1(СПК-2) УМЕТЬ провести анализ исходных данных для проектиро-

	вания подсистем и средств обеспечения информационной безопасности В1(СПК-2) ВЛАДЕТЬ Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3)	З1 (ОПК-3) ЗНАТЬ принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности У1(ОПК-3) УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.
Способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	З1(ОПК-1) ЗНАТЬ научные задачи в области обеспечения информационной безопасности

(ОПК-1);	У1(ОПК-1) УМЕТЬ: применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность В1(ОПК-1) ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность
Владение современными методами построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также методами разработки и реализации алгоритмов их решения на основе фундаментальных знаний в области математики и информатики (ПК-1)	З1 (ПК-1) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-1) УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения

	В1 (ПК-1) ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения
Способность разрабатывать и реализовывать алгоритмы организации работы современных вычислительных комплексов и компьютерных сетей (ПК-2)	З1 (ПК-2) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-2) УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения В1 (ПК-2) ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

24 часов составляет контактная работа с преподавателем – 22 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часа мероприятий текущего контроля успеваемости, 0 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

84 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по компьютерным сетям, дискретной математике и основам кибернетики в объеме, соответствующем основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используется программный пакет Beamer для подготовки слайдов лекций в среде LaTeX, программное средство просмотра pdf-файлов Adobe Reader, программное средство просмотра презентаций MS Power Point 2016.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются следующие темы:

1. Основы математического аппарата квантовой информатики, основные понятия классической теории информации.
2. Основные протоколы квантовой передачи и переработки информации, основные протоколы квантовой криптографии.
3. Основные экспериментальные реализации протоколов квантовой криптографии.
4. Методы и способы доказательств секретности ключей в системах квантового распределения ключей.

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	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	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др)*	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п..	Всего
Тема 1. 1. Основы математического аппарата квантовой информатики, основные понятия классической теории информации. Что такое квантовая криптография, и какие задачи она решает. Одноразовые ключи. Критерий Шеннона абсолютной секретности. Существующие достижения в квантовой криптографии. Основы математического аппарата квантовой информатики: описание квантовых состояний отдельных и составных квантовых систем, чистые, смешанные состояния, квантовая запутанность, ортогональные и обобщенные измерения, очищение квантовых	6	2	-	-	-		2	4	-	4

состояний, теорема о запрете копирования, преобразования квантовых систем, вполне положительные отображения. Меры близости квантовых состояний, используемые в протоколах квантовой криптографии. Основные понятия классической теории информации. Энтропии Шеннона, Реньи и их свойства. Условная, взаимная информация, типичные последовательности, теоремы кодирования источника, прямая и обратная теоремы кодирования для канала с шумом, пропускная способность										
Тема 2. Основные протоколы квантовой передачи и переработки информации, основные протоколы квантовой криптографии. Энтропия фон Неймана, основные свойства и использование в квантовой теории информации. Понятие квантовых каналов связи. Классическая пропускная способность квантового канала связи. Индивидуальные и коллективные измерения в квантовой криптографии. Фундаментальная граница Холево для достижимой границы классической информации. Множественность атак подслушивателя, связь атак с пропускными способностями квантового канала. Основные свойства квантовых энтропий Реньи (min и max энтропий). Сглаженные min и max энтропии, цепочечные правила, изменение min и max энтропий при	26	6	-	-	-	-	6	-	20	20

действии супероператора, свойства min и max энтропии для составных квантовых систем. Энтропийные соотношения неопределенностей в квантовой криптографии, связь с min и max энтропиями Реньи										
Тема 3. Основные экспериментальные реализации протоколов квантовой криптографии Основные протоколы квантовых коммуникаций и их описание: квантовая телепортация, сверхплотное кодирование, квантовое распределение ключей. Основные протоколы квантового распределения ключей: BB84, B92, E91, SARG04, фазово-временное кодирование, дифференциально-фазовое кодирование, релятивистское квантовое распределение ключей через открытое пространство с синхронизацией и без синхронизации часов на приемной и передающей стороне.	32	12	-	-	-	-	12	20	-	20
Тема 4. Методы и способы доказательств секретности ключей в системах квантового распределения ключей Критерий секретности ключей в квантовой криптографии, основанный на следовом расстоянии. Универсальные хэш-функции второго рода, использование в процедурах усиления секретности. Теорема об остатке хэширования	42	2	-	-	-	-	2	30	10	40

(Left over hash Lemma). Доказательство секретности квантового распределения ключей на примере протокола BB84, основанное на энтропийных соотношениях неопределенностей (случай строго однофотонного источника информационных состояний). Анализ криптографической 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 измерениями с определенным исходом, прозрачная атака со светоделителем. Модификация протоколов квантовой криптографии с учетом атак, связанных с не строгой однофотонностью источника информационных состояний. Пример – метод с состояниями ловушками (Decoy State метод). Связь квантового критерия секретности, основанного на следовом расстоянии, с критерием Шеннона, основанном на сложности перебора.										
5. Промежуточная аттестация – устный экзамен	2	2						0		
Итого	108	24						84		

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

Учебно-методическое и информационное обеспечение.

1) А.С.Холево. Квантовые системы, каналы, информация, Москва. МЦМО, сс.327 (2010); A. S. Holevo, Introduction to Quantum Information Theory}, (MTNMO, Moscow, 2002) [in Russian]; Usp. Mat. Nauk, {\bf 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); R. G. Gallager, Information Theory and Reliable Communication,

(Wiley, New York, 1968)

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

7) C.H.Bennett, G.Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 175 (1984).

8) C.H.Bennett, Phys. Rev. Lett., 68, 3121 (1992).

9) R.Renner, Security of Quantum Key Distribution, PhD Thesis, ETH Z\"urich, Dec. 2005. arXiv/quant-ph: 0512258.

10) V.Scarani, H.Bechmann-Pasquinucci, N.J.Cerf, M.Dusek, N.Lutkenhaus, M.Peev, Rev. Mod. Phys., 81, 1301 (2009).

10) D.Mayers, Journal ACM, 48 351 (2001).

12) H.-K.Lo, H.F.Chau, Science, 283 2050 (1999).

13) P.Shor, J.Preskill, Phys. Rev. Lett., 85 441 (2000).

14) M.Koashi, J. Phys. Conf. Ser., 36, 98 (2006).

15) M.Tomamichel. R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.

16) M.Tomamichel, C.Ci Wen Lim, N.Gisin, R.Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv/quant-ph: 11034130.

17) С.П.Кулик, А.П.Маккавеев, С.Н.Молотков, Письма в ЖЭТФ. 85, 354 (2007).

18) С.Н.Молотков, ЖЭТФ. 133, 5 (2008).

19) Д.А.Кронберг, С.Н.Молотков, ЖЭТФ, 136, 650 (2009); ЖЭТФ, 138, 33 (2010).

20) H.P.Robertson, Phys. Rev., 34, 163 (1929).

21) D.Deutsch, Phys. Rev. Lett., 50, 631 (1983).

22) K.Kraus, Phys. Rev., D 35, 3070 (1987).

23) H.Maassen, J.B.M.Uffink, Phys. Rev. Lett., {\bf 60}, 1103 (1988).

24) J.M.Renes, J.-C. Boileau, Phys. Rev. Lett., 103, 020402-1 (2009).

25) 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.

26).M.Cover J.A.Thomas. Elements of Information Theory. Wiley, (1991).

27) M.Berta, M.Christandl, R.Colbeck, J.M.Renes, R.Renner, Nature Physics, 6, 659 (2010).

28) M.Tomamichel, R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.

29) J.M.Renes, R.Renner, One-Shot Classical Data Compression with Quantum Side Information and the Distillation of Common Randomness or Secret Keys, arXiv/quant-ph: 10080452.

30) J.L.Carter, M.N.Wegman Universal Classes of Hash Functions, J. Comp. Syst. Sci., 18, (1979) 143.

31) M.N.Wegman, J.L.Carter, New Hash Functions and Their Use Authentication and Set Euqality, J. Comp. Syst. Sci., 22, 265 (1991).

32) C.H.Bennett, G.Brassard, C.Crepeau, U.M.Maurer, Generalized Privacy Amplication, IEEE Trans. on Inf. Theory, 41 (1995) 1915.

33)M.Tomamichel, C.Schaffner, A.Smith, R.Renner, Leftover Hashing Against Quantum Side Information, arXiv/quant-ph: 10022436.

34) 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).

35)W.Hoeffding, Probability Inequalities for Sums of Bounded Random Variables, J. Amer. Statistical Assoc., 58 (1963) 13.

36) R. J. Serfling, Probability Inequalities for the Sum in Sampling without Replacement ,Ann. Stat., 2 (1974) 39.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1) Основной Интернет-ресурс по квантовой информатике xxx.lanl.gov\quant-ph

2) http://www.aps.org – журналы Американского физического общества,

jetpletters.ac.ru, jetp.ac.ru – журналы Российской академии наук.

Информационные технологии, используемые в процессе обучения

1. Программный пакет Beamer для подготовки слайдов лекций в среде LaTeX

2. Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
3. Программное обеспечение для создания и просмотра презентаций MS Power Point

Активные и интерактивные формы проведения занятия

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия
1	Лекция 11	Лекция-конференция на тему «Использование различных протоколов дл квантового распределения ключей»

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской и проектором.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

д.ф.-м.н. Молотков Сергей Николаевич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Математические методы квантовой криптографии»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю) *(критерии и показатели берутся из соответствующих карт компетенций, при этом пользуются либо традиционной системой оценивания, либо БРС)*					ОЦЕНОЧНЫЕ СРЕДСТВА
	1	2	3	4	5	
	Неудовлетворительно	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично	
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности 31 (ОПК-3)	Отсутствие знаний	Фрагментарные представления о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	В целом сформированные, но неполные знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные систематические знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Устный экзамен
УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и	Отсутствие умений	Фрагментарные умения обоснования степени соответствия защищаемых объектов информатизации	В целом успешное, но не систематическое умение обоснования степени соответ-	Успешное, но содержащее отдельные пробелы умение обоснования степени соответ-	Сформированное умение обоснования степени соответствия защищаемых объектов информатизации	Контрольные работы

информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)		и информатизационных систем действующим стандартам в области информационной безопасности.	ствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	ствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	и информатизационных систем действующим стандартам в области информационной безопасности.	
ЗНАТЬ: современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения З1 (ПК-1)	Отсутствие знаний	Фрагментарные представления о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	В целом сформированные, но неполные знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные, но содержащие отдельные пробелы знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные систематические знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Устный экзамен
УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и	Отсутствие умений	Фрагментарные умения применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и	В целом успешное, но не систематическое умение применять современные методы построения и анализа математических моделей, возникающих при решении ес-	Успешное, но содержащее отдельные пробелы умение применять современные методы построения и анализа математических моделей, возникающих при	Сформированное умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и	Контрольные работы

реализации алгоритмов их решения У1 (ПК-1)		реализации алгоритмов их решения	тественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	реализации алгоритмов их решения	
ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения В1 (ПК-1)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	В целом успешное, но не полное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	Сформированное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	Контрольные работы, реферат
ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код З1 (ПК-2)	Отсутствие знаний	Фрагментарные представления о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом сформированные, но неполные знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и	Сформированные, но содержащие отдельные пробелы знания о современных методах разработки и реализации алгоритмов организации работы вычислительных	Сформированные систематические знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего по-	Устный экзамен

			компьютерных сетей последнего поколения	комплексов и компьютерных сетей последнего поколения	коления	
УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код У1 (ПК-2)	Отсутствие умений	Фрагментарные умения применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не систематическое умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированное умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код В1 (ПК-2)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не полное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
ЗНАТЬ: научные задачи в об-	Отсутствие знаний	Фрагментарные представления о на-	В целом сформированные, но не-	Сформированные, но содержащие	Сформированные систематические	Устный экзамен

ласти обеспечения информационной безопасности З1(ОПК-1)		учных задачах в области обеспечения информационной безопасности	полные знания о научных задачах в области обеспечения информационной безопасности	отдельные пробелы о научных задачах в области обеспечения информационной безопасности	знания о научных задачах в области обеспечения информационной безопасности	
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Устный экзамен
ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность В1(ОПК-1)	Отсутствие навыков	Фрагментарное владение навыками внедрения полученных результатов в практическую деятельность	В целом успешное, но не полное владение навыками внедрения полученных результатов в практическую деятельность	Успешное, но содержащее отдельные пробелы владение навыками внедрения полученных результатов в практическую деятельность	Сформированное владение навыками внедрения полученных результатов в практическую деятельность	устный экзамен
ЗНАТЬ Средства обеспече-	Отсутствие знаний	Фрагментарные представления о средствах обеспече-	В целом сформированные, но неполные знания о	Сформированные, но содержащие отдельные пробе-	Сформированные систематические знания о средствах	Устный экзамен

ния информационной безопасности З1(СПК-2)		ния информационной безопасности	средствах обеспечения информационной безопасности	лы о средствах обеспечения информационной безопасности	обеспечения информационной безопасности	
УМЕТЬ провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности У1(СПК-2)	Отсутствие умений	Фрагментарные умения проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но не систематическое умение проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Успешное, но содержащее отдельные пробелы проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Сформированное умение проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Устный экзамен
ВЛАДЕТЬ Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности В1(СПК-2)	Отсутствие навыков	Фрагментарное владение Навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но не полное владение навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Успешное, но содержащее отдельные пробелы владение навыками навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Сформированное владение навыками навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Устный экзамен

Фонды оценочных средств, необходимые для оценки результатов обучения

Каждый учащийся в процессе обучения готовит научный проект, который заключается в построении системы квантового распределения ключей (КРК), на основе какого-либо протокола. Для построенной системы КРК должны быть указаны:

1) Протокол
2) Тип кодирования – фазовое, поляризационное, фазово-временное
3) Критическая длина линии для гарантированного распределения секретных ключей
4) Описываются возможные типа атак на криптосистему, известные из открытых источников.
5) Устойчивость к известным атакам на данный тип системы КРК

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

Система контроля и оценивания

За выполнение научной работы выставляются баллы. Оценивается:

1) Полнота описания протокола КРК (<=1 балл)
2) Корректность описания КРК (<=1 балл)
3) Корректность получения оценок секретности ключей (<=1 балл)
4) Полнота описания возможных атак (<= 1 балл)
5) Библиография, посвящённая исследованию такого типа криптосистем (<= 1 балл).

По каждому параметру выставляется, которая равна доле полноты/корректности параметра. Далее все баллы суммируются и округляются. Полученная значение является итоговой оценкой.

Пример: 1) 1 2) 1 3) 0,7 4) 0,2 5) 1, в итоге

1 + 1 + 0, 7 + 0,2 + 1 = 3,7 -> оценка 4 (“хорошо”).

Структура и график контрольных мероприятий

Защита научной работы в конце семестра.