ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ ПРИКЛАДНЫХ МАТЕМАТИЧЕСКИХ ИССЛЕДОВАНИЙ
КАРЕЛЬСКОГО НАУЧНОГО ЦЕНТРА
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИПМИ КарНЦ РАН)

УТВЕРЖДАЮ
Директор ИПМИ КарНЦ РАН
д.ф.-м.н., проф.
_____ В.В. Мазалов
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Направление подготовки: 01.06.01 «Математика и механика»
Профиль: Дискретная математика и математическая кибернетика
Квалификация: Исследователь. Преподаватель-исследователь

Петрозаводск
2017

Составитель рабочей программы:

г.н.с., профессор, д.ф.-м.н. _____ Ю.Л. Павлов
(должность, ученое звание, ученая степень) (подпись) (Ф.И.О.)

Рабочая программа составлена в соответствии с ФГОС ВО (уровень подготовки кадров высшей квалификации) и утверждена на заседании Ученого совета ИПМИ КарНЦ РАН

«16» марта 2017 г., протокол № 3

Председатель Ученого совета
Д.ф.-м.н., проф. _____ В.В. Мазалов

1. Цели и задачи дисциплины

1.1. *Целью дисциплины является*: получение базовых знаний математических основ криптографии и криптоанализа; формирование навыков использования методов криптологии в научно-исследовательской и педагогической деятельности; повышение квалификации в области научных основ и применения методов криптологии для решения фундаментальных и прикладных научно-технических проблем.

1.2. *Виды профессиональной деятельности*:

- научно-исследовательская деятельность;
- проектная деятельность.

Выпускник, освоивший программу аспирантуры в соответствии с данными видами профессиональной деятельности, готов решать следующие профессиональные задачи:

- подготовка научных и научно-технических публикаций;
- разработка алгоритмов с использованием методов криптологии;
- использование математических методов криптологии в научно-исследовательской, педагогической и производственно-технологической деятельности, включая разработку алгоритмических и программных решений в области прикладного программирования.

2. Место дисциплины в структуре ООП аспиранта

Дисциплина «Математические основы криптологии» является вариативной согласно учебному плану ООП по направлению подготовки 01.06.01 «Математика и механика», профиль – Дискретная математика и математическая кибернетика. Дисциплина изучается в 1-м и 2-м семестрах, направлена на формирование компетенций УК1, УК3, УК4, ОПК1, ОПК2, ПК1, ПК4.

3. Требования к уровню подготовки аспиранта, завершившего изучение дисциплины

В результате освоения дисциплины аспирант приобретает следующие компетенции.

Компетенция	**Код по ФГОС ВО (уровень подготовки кадров)**	**Структура компетенции**	**Дескрипторы (уровни) - основные признаки освоения (показатели достижения результата)**		**Формы и методы обучения, способствующие формированию и развитию компетенции**
Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	УК1	Знать: классические методы криптологии и текущее состояние современных научных достижений, фундаментальные основы криптологии	Высокий (превосходный) уровень	Знать: основные понятия, модели, алгоритмы и теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы криптоанализа	
			Пороговый (базовый) уровень	основные принципы криптологии	
		Уметь: генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Высокий (превосходный) уровень	Уметь: генерировать новые идеи при решении исследовательских и практических задач	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать методы криптоанализа в научных исследованиях	
			Пороговый (базовый) уровень	решать практические задачи криптографии	
		Владеть: способностью к анализу и оценке	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской

		современных научных достижений	Повышенный (продвинутый) уровень	навыками криптоанализа	деятельности, применение полученных знаний для решения практических задач
			Пороговый (базовый) уровень	основными методами криптографии	
Готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач	УК3	Знать: текущее состояние современных научных достижений	Высокий (превосходный) уровень	Знать: основные понятия, методы, алгоритмы и теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы криптоанализа	
			Пороговый (базовый) уровень	основные принципы криптологии	
		Уметь: вести научно-исследовательскую деятельность	Высокий (превосходный) уровень	Уметь: применять полученные теоретические знания для решения новых практических задач	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать методы криптоанализа в научных исследованиях	
			Пороговый (базовый) уровень	решать практические задачи	
		Владеть: организационными, коммуникативными навыками, позволяющими осуществлять работу	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для
			Повышенный (продвинутый) уровень	навыками использования методов криптоанализа	

		в исследовательских коллективах	Пороговый (базовый) уровень	методикой решения практических задач	решения практических задач
Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	УК4	Знать: текущее состояние современных научных достижений	Высокий (превосходный) уровень	Знать: основные понятия, модели, алгоритмы и теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы криптоанализа	
			Пороговый (базовый) уровень	основные принципы криптологии	
		Уметь: принимать мотивированное решение	Высокий (превосходный) уровень	Уметь: применять полученную теоретическую подготовку для постановки и решения практических задач с использованием русского и английского языков	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать методы криптоанализа в научных исследованиях с использованием русского и английского языков	
			Пороговый (базовый) уровень	решать конкретные задачи	
		Владеть: навыками принятия решений и способностью нести	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской

		ответственность за принятые решения	Повышенный (продвинутый) уровень	навыками использования методов криптоанализа	деятельности, применение полученных знаний для решения практических задач
			Пороговый (базовый) уровень	навыками использования методов криптографии	
Способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий	ОПК1	Знать: текущее состояние современных научных достижений в области криптологии	Высокий (превосходный) уровень	Знать: основные понятия, модели, алгоритмы и теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы криптоанализа	
			Пороговый (базовый) уровень	методику использования методов криптографии	
		Уметь: использовать основные методы криптологии	Высокий (превосходный) уровень	Уметь: применять полученную теоретическую подготовку для решения новых практических задач	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать методы криптоанализа в научных исследованиях	
			Пороговый (базовый) уровень	решать конкретные практические задачи	
		Владеть: навыками и основными методами криптологии	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	навыками использования основных методов криптоанализа	

			Пороговый (базовый) уровень	навыками использования основных методов криптографии	
Готовность к преподавательской деятельности по основным образовательным программам высшего образования	ОПК2	Знать: историю развития криптологии, классические методы и текущее состояние современных научных достижений в области защиты информации	Высокий (превосходный) уровень	Знать: теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	историю развития криптологии и основные методы криптоанализа	
			Пороговый (базовый) уровень	основные принципы криптологии	
		Уметь: применять полученные теоретические знания в преподавательской деятельности	Высокий (превосходный) уровень	Уметь: разрабатывать новые учебные программы по криптологии	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать полученные знания при проведении учебных занятий по криптологии в качестве преподавателя	
			Пороговый (базовый) уровень	объяснить ход решения конкретных практических задач	
		Владеть: способностью к критическому анализу учебных программ по криптологии	Высокий (превосходный) уровень	Владеть: основными методами разработки учебных программ по криптологии	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	навыками объяснения сути основных методов криптологии	
			Пороговый (базовый) уровень	основными методами криптологии	

Понимание роли и места дискретной математики и математической кибернетики в математике в целом, их связи с другими разделами математики и другими областями науки	ПК1	Знать: методы дискретной математики, теории графов, алгебры и теории алгоритмов, применяемые в криптологии и задачи защиты информации, решаемые с помощью криптографических протоколов	Высокий (превосходный) уровень	Знать: основные теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы дискретной математики, теории графов, теории алгоритмов и криптографические протоколы, используемые в криптоанализе	
			Пороговый (базовый) уровень	основные методы дискретной математики и теории алгоритмов, используемые в криптографии	
		Уметь: оценивать методы дискретной математики и математической кибернетики с точки зрения возможности и целесообразности их применения в криптологии	Высокий (превосходный) уровень	Уметь: применять полученные теоретические знания для решения новых научно-исследовательских и практических задач	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать методы дискретной математики и математической кибернетики в научных исследованиях в области криптологии	
			Пороговый (базовый) уровень	решать конкретные практические задачи	
		Владеть: навыками использования методов дискретной математики	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской

		и математической кибернетики в криптологии	Повышенный (продвинутый) уровень	навыками использования методов криптоанализа	деятельности, применение полученных знаний для решения практических задач
			Пороговый (базовый) уровень	основными методами криптографии	
Способность применять алгебраические, логические, комбинаторные, вероятностные и алгоритмические методы анализа графов, автоматов, формальных языков, символьных последовательностей	ПК4	Знать: текущее положение современных научных достижений в дискретной математике и математической кибернетике, классическую и современную методологию криптологии	Высокий (превосходный) уровень	Знать: основные теоретические положения курса «Математические основы криптологии»	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение знаний для решения практических задач
			Повышенный (продвинутый) уровень	основные методы дискретной математики и математической кибернетики, применяемые в криптоанализе	
			Пороговый (базовый) уровень	Историю развития криптологии и основые методы дискретной математики, теории графов, теории вероятностей и теории алгоритмов, применяемые в криптографии	
		Уметь: применять алгебраические, логические, комбинаторные, вероятностные, алгоритмические и теоретико-графовые методы при решении задач защиты информации	Высокий (превосходный) уровень	Уметь: применять полученные теоретические знания для решения новых практических задач	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	эффективно использовать иетоды дискретной математики и математической кибернетики в научных исследованиях	

			Пороговый (базовый) уровень	решать конкретные практические задачи	
		Владеть: навыками использования методов дискретной математики и математической кибернетики при решении задач защиты информации	Высокий (превосходный) уровень	Владеть: основными методами научных исследований	Посещение лекций, семинаров, участие в научно-исследовательской деятельности, применение полученных знаний для решения практических задач
			Повышенный (продвинутый) уровень	навыками использования методов дискретной математики и математической кибернетики в криптологии	
			Пороговый (базовый) уровень	основными методами алгебры, логики, комбинаторики, теории графов, теории вероятностей и теории алгоритмов, используемые в криптографии	

4. Объем дисциплины и виды учебной работы

4.1. *Объем дисциплины*

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

Вид учебной работы	Объем часов / зачетных единиц
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
лекции	16
семинары	-
практические занятия	16
Самостоятельная работа аспиранта (всего)	36
Вид контроля по дисциплине	зачет/экзамен, 4

4.2. *Лекционные занятия*

№ темы	Название раздела/темы дисциплины	Технология проведения	Формируемые компетенции (код)	Форма оценочных средств	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Чтение лекций, использование учебников, методических пособий и УМК	УК 3	коллоквиум	3
2	Алгебра секретных систем. Чистые шифры	Чтение лекций, использование учебников, методических пособий и УМК	ПК 1	собеседование	4
3	Совершенно секретные системы	Чтение лекций, использование учебников, методических пособий и УМК	ОПК 1	коллоквиум	3
4	Современные методы криптологии. Секретные системы с открытым ключом	Чтение лекций, использование учебников, методических пособий и УМК	ОПК 2	собеседование	4

5	Криптографические протоколы	Чтение лекций, презентации с использованием мультимедийного оборудования, использование учебников, методических пособий и УМК	ПК 4	коллоквиум	2
	Итого:				**16**

4.3. *Практические* (*семинарские*) *занятия*

№ темы	Тематика занятий	Технология проведения	Формируемые компетенции (код)	Форма оценочных средств	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Лабораторный практикум, консультация по решению задач	УК 1	Дискуссия	3
2	Алгебра секретных систем. Чистые шифры	Лабораторный практикум, консультация по решению задач	УК 4	Дискуссия	3
3	Совершенно секретные системы	Лабораторный практикум, консультация по решению задач	ОПК 1	Дискуссия	4
4	Современные методы криптологии. Секретные системы с открытым ключом	Лабораторный практикум, консультация по решению задач	ОПК 2	Дискуссия	3
5	Криптографические протоколы	Лабораторный практикум, консультация по решению задач	ПК 1	Дискуссия	3
	Итого:				**16**

5. Содержание дисциплины

Тема №1. Понятие криптологии, терминология, исторический очерк.

Понятие криптологии и ее структура (криптография, криптоанализ, стеганография). История криптографии от древности до нашего времени. Примеры шифров. Понятие секретной системы по Шеннону. Представление секретных систем в виде графов. Критерии качества секретных систем

Тема №2. Алгебра секретных систем. Чистые шифры.

Операции над секретными системами (взвешенное суммирование и произведение). Ассоциативность операций. Коммутирующие шифры. Эндоморфные шифры. Множество эндоморфных шифров как ассоциативная алгебраическая система с двумя операциями. Определение чистого шифра. Смешанные шифры. Свойства чистых шифров. Остаточные классы сообщений и криптограмм. Методы криптоанализа чистых шифров. Подобие секретных систем.

Тема №3. Совершенно секретные системы.
Определение и свойства совершенно секретных систем. Доказательство существования совершенно секретных систем. Гаммирование. Энтропия. Ненадежность. Энтропийные методы криптоанализа и примеры. Стандарты криптосистем.

Тема №4. Современные методы криптологии. Секретные системы с открытым ключом.
Элементы теории алгоритмов, сложность алгоритма. Односторонние функции. Функции с секретом. Понятие секретной системы с открытым ключом. Секретная система RSA. Примеры функций, похожих на функции с секретом. Разложение натурального числа на простые сомножители. Дискретное логарифмирование. Изоморфизм графов. Рюкзачный метод шифрования.

Тема №5. Криптографические протоколы.
Понятие криптографического протокола. Протокол выработки общего ключа. Протоколы аутентификации. Подписание контракта. Подбрасывание монеты. Электронная подпись. Электронные деньги. Протокол византийского соглашения. Разделение секрета. Функции хэширования.

6. Учебно-методическое обеспечение самостоятельной работы аспирантов

Формы проведения самостоятельной работы

№	Тема дисциплины	Форма самостоятельной работы	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	4
2	Алгебра секретных систем. Чистые шифры	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	7
3	Совершенно секретные системы	Выполнение домашних и контрольных работ с привлечением специальной научно-технической литературы и программных средств и интернет-ресурсов. Участие в НИР аспирантов	9
4	Современные методы	Выполнение домашних и контрольных	9

	криптологии. Секретные системы с открытым ключом	работ с привлечением специальной научно-технической литературы и программных средств и интернет-ресурсов. Участие в НИР аспирантов	
5	Криптографические протоколы	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	7
	Итого:		36

7. Контроль знаний аспирантов

7.1. *Формы текущего контроля работы аспирантов*:

1) коллоквиум; 2) собеседование; 3) дискуссия.

7.2. *Промежуточная аттестация по дисциплине*:

проводится в форме зачета/экзамена.

7.3. Вопросы по дисциплине «Математические основы криптологии»

1. Криптология, ее структура, цели и задачи.
2. Шифры Цезаря и Сцитала.
3. Шифры Энея.
4. Шифры Третимия.
5. Дисковые шифры.
6. Шифры Кардано.
7. Шифр Виженера.
8. Шифры Бофора.
9. Шифратор Джеферсона.
10. Шифры Кеплера и Галилея.
11. История отечественной криптографии.
12. Шифровальная машина «Энигма».
13. Шифры подстановки и методы их вскрытия.
14. Шифры транспозиции и методы их вскрытия.
15. Алгебра секретных систем.
16. Чистые и смешанные шифры.
17. Метод характерных слов.
18. Совершенная секретность.
19. Доказательство существования совершенно секретного шифра.
20. Шифр Вернама и гаммирование.
21. Датчики псевдослучайных чисел и криптография.
22. Энтропия и надежность шифров.
23. Криптосистемы с открытым ключом.
24. Односторонние функции и функции с секретом.
25. Система RSA.
26. Сложность криптографических алгоритмов.
27. Дискретное логарифмирование.
28. Задача о рюкзаке.
29. Изоморфизм графов и криптография.
30. Криптографические протоколы.
31. Протоколы аутентификации.

32. Открытое распределения ключей.
33. Математика разделения секрета.
34. Электронная подпись
35. Электронные деньги.

7.4. Критерии оценки промежуточной аттестации аспирантов по дисциплине «Математические основы криптологии»

Критерии оценки экзамена	
оценка «отлично»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы. Грамотно использует научную лексику, свободно ориентируется в материале курса. Аспирант успешно справляется с практическим заданием.
оценка «хорошо»	Ставится, если аспирант строит ответ в соответствии с планом, обнаруживает понимание теоретических вопросов. Ответ содержит ряд несущественных неточностей. Наблюдается неточность при ответе на дополнительные вопросы. Аспирант успешно справляется с практическим заданием или допускает незначительные ошибки.
оценка «удовлетвори-тельно»	Ставится, если ответ аспиранта недостаточно логически выстроен, обнаруживается недостаточно полное понимание теоретических вопросов, хотя основные понятия раскрываются правильно. Аспирант справляется с практическим заданием, допуская ошибки.
оценка «неудовлетво-рительно»	Ставится если, аспирант оказывается неспособным правильно раскрыть содержание основных понятий. Проявляет стремление подменить научное обоснование проблемы общими рассуждениями. Ответ содержит ряд серьезных неточностей. Аспирант не способен выполнить практическое задание.

Критерии оценки зачета	
«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы. При ответе грамотно использует научную лексику, свободно ориентируется в материале курса. Аспирант успешно справляется с практическим заданием.
«не зачтено»	Ставится если, аспирант оказывается неспособным правильно раскрыть содержание основных понятий, плохо ориентируется в материале курса. Ответ содержит ряд серьезных неточностей. Аспирант не способен выполнить практическое задание.

7.5. Фонд оценочных средств

Содержание фонда оценочных средств: см. Приложение №1.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Ю.С. Харин и др. Криптология: учебник. Минск, БГУ, 2013.
2. Введение в криптографию. Под редакцией В. В. Ященко. Москва, МЦНМО, 2012.
3. А.В. Бабаш, Г.П. Шанкин. Криптография. Москва, СОЛОН-Р, 2002.

8.2. Дополнительная литература

1. Х.К. Тилберг. Основы криптологии. Профессиональное руководство и интерактивный учебник. Москва, Мир, 2006.
2. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. Математические и компьютерные основы криптологии. Минск, Новое знание, 2003.
3. Введение в криптографию. Под. редакцией В.В. Ященко. Москва, МЦНМО, 1999.
4.А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии, Москва, Гелиос АРВ, 2005.
5. Р.В. Воронов. Введение в теоретико-числовые алгоритмы асимметричной криптографии. Петрозаводск, ПетрГУ, 2006.
6. Н. Смарт. Криптография. Москва, Техносфера, 2006.
7. В.М. Фомичев. Дискретная математика и криптология. Курс лекций. Москва, Диалог-МИФИ, 2003.

8.3.

Интернет-ресурсы	
www.garant.ru	Базы данных, информационно-справочные и поисковые системы
http://biblioclub.ru	Университетская библиотека Online
http://www.elibrary.ru	Электронная библиотека
http://ndce.edu.ru	Каталог учебников, электронных ресурсов для высшего образования
http://edu.ru	Федеральный портал «Российское образование»
http://window.edu.ru	Портал «Единое окно доступа к образовательным ресурсам»
http://school.edu.ru	Российский общеобразовательный портал
http://www.enlignt.ru/crypto/articles/shannon/shann_i.htm	Книга К. Шеннон «Теория связи в секретных системах»

http://cryptography.ru	Сайт МГУ «Математическая криптография
http://www.youtube.com/watch?v=Z0bsnutajAo	Лекция «Введение в криптографию»

9. Перечень программного обеспечения

Mathematica, PGP, Криптограф, LaTeX, Word

10. Материально-техническое обеспечение дисциплины

Аудитории для проведения лекционных и практических занятий,
мультимедийное оборудование, доска, доступ к Интернет-ресурсам.

11. Особенности организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья

Обучение инвалидов и лиц с ограниченными возможностями осуществляется в соответствии со следующими документами.
1. Ст.79, 273-ФЗ «Об образовании в Российской Федерации» .
2. Раздел IV, п.п. 46-51 приказа Минобрнауки России от 19.11.2013 № 1259 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам подготовки научно-педагогических кадров в аспирантуре (адъюнктуре)».
3. Методические рекомендации по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса (утверждены зам. Министра образования и науки РФ А.А.Климовым от 8.4.2014 г. № АК-44/05 вн).

Приложение 1

Содержание фонда оценочных средств

Коллоквиум

Вопросы к коллоквиуму по дисциплине
«Математические основы криптологии»:

1. Понятие криптологии. Криптография. Криптоанализ. Стеганография.
2. Шифр Цезаря. Шифр сцитала. Шифры Энея. Книжные шифры. N-граммное шифрование. Шифры подстановки. Шифры транспозиции.
3. Дисковые шифры. Блочное шифрование. Шифры Третимия. Многоалфавитное и блочное шифрование.
4. Шифры Виженера, Бофора, Вернаама. Гаммирование. Шифровальная машина «Энигма».
5. Понятие и свойства секретных систем. Критерии оценки секретных систем.
6. Совершенно секретные системы. Энтропия. Ненадежность. Примеры расшифровки энтропийным методом.
7.Экстремальные задачи. Выпуклый анализ. Экстремальные задачи в евклидовых пространствах. Линейное и выпуклое программирование. Задачи на минимакс.
8. Криптографические протоколы. Примеры.
9.. Протоколы открытого обмена ключами.
10. Протоколы аутентификации и электронной подписи.
11. Электронные деньги. Неотслеживаемость.
12. Протоколы разделения секрета. Примеры.

Критерии оценки коллоквиума

«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий. Ответ содержит ряд серьезных неточностей. Аспирант не отвечает на дополнительные вопросы.

Собеседование

Тема №2. Алгебра секретных систем. Чистые шифры.

Операции над секретными системами. Взвешенное суммирование. Произведение. Ассоциативность операций. Эндоморфизм шифров. Множество шифров как алгебраическая система. Чистые и смешанные шифры. Свойства чистых шифров.

Коммутирующие шифры. Остаточные классы сообщений и криптограмм. Метод характерных слов. Методы криптоанализа шифров транспозиции и Виженера.

Тема №4. Современные методы криптологии. Секретные системы с открытым ключом

Односторонние функции. Функции с секретом. Сложность алгоритмов. Идея секретных систем с открытым ключом. Система RSA. Разложение натурального числа на простые сомножители. Дискретное логарифмирование.

Критерии оценки собеседования

«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы. При ответе грамотно использует научную лексику, способен привести примеры, демонстрирующие эффективность теории.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий. Ответ содержит ряд серьезных неточностей. Аспирант не отвечает на дополнительные вопросы и не ориентируется свободно в излагаемом материале.

Дискуссия

Темы дискуссий

1. Криптография и криптоанализ.
2. Криптография и стеганография.
3. Основные идеи древних шифров.
4. Криптография средневековья.
5. Дисковое шифрование.
6. Множество шифров как алгебраическая система.
7. Стойкость чистых шифров.
8. Основная задача криптоаналитика.
9. Можно ли создать абсолютно стойкий шифр?
10. Секретные системы с открытым ключом.
11. Стойкость асимметричных секретных систем.
12. Надежность электронной подписи.
13. Электронные деньги и неотслеживаемость.
14. Протоколы типа византийского соглашения.

Критерии оценки дискуссии:

«зачтено»	Ставится, если аспирант раскрывает тему дискуссии логично, обнаруживает глубокое знание темы. Уверенно отвечает на вопросы, грамотно обосновывает свою позицию. При ответе свободно и уверено ориентируется в материале.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий по теме дискуссии. Ответ содержит ряд серьезных неточностей. Аспирант не раскрывает тему дискуссии, не обосновывает свою позицию по теме дискуссии.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ В РАБОЧЕЙ ПРОГРАММЕ

за _____/_____ учебный год

В рабочую программу _____
(наименование дисциплины)

Для специальности (тей) _____
(номер специальности)

Вносятся следующие дополнения и изменения:

Дополнения и изменения внес _____
(должность, ФИО, подпись)

Рабочая программа пересмотрена и одобрена на заседании Ученого совета ИПМИ КарНЦ РАН

«___» _____ 20___ г.

Председатель Ученого совета _____ _____
(подпись) (ФИО)