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 _____ Е.И. Моисеев

«____» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Криптосистемы с открытым ключом»

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)

2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Информационная безопасность компьютерных систем

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 дисциплинам вариативной части образовательной программы и является обязательной для освоения во 2-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
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	З1(ОПК-1) ЗНАТЬ

информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);	научные задачи в области обеспечения информационной безопасности 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
Способность планировать и решать задачи собственного профессионального	З1(УК-5(6)) ЗНАТЬ:

и личностного развития (УК-5(6))	содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда. У1(УК-5(6)) УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.
Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1)	У2 (УК-1) УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений В2(УК-1) ВЛАДЕТЬ: навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач, в том числе в междисциплинарных областях

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

40 часов составляет контактная работа с преподавателем – 32 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 4 часа мероприятий текущего контроля успеваемости, 2 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

68 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по основам алгебры и теории чисел, а также теории алгоритмов в объеме, соответствующем основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика» и/или 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используется программное обеспечение для подготовки слайдов лекций MS PowerPoint.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные проблемы и задачи, связанные с обеспечением информационной безопасности. Рассматриваются понятия евклидовости, факториальности, свойства делимости и их применения, простоты в произвольном кольце, а также конкретизируются понятия аутентификации, достоверной и слепой подписи, электронных денег. Рассматриваются протоколы на основе алгебраической теории чисел.

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. Алгебраические основы теории делимости	23	12	-	2	-	1	15	8	-	8

Основные понятия и термины. Понятие евклидового кольца, простого элемента в произвольном кольце, единиц и ассоциированных элементов, факториального кольца. Доказываются теоремы об однозначности разложения на простые множители в кольце целых чисел, в произвольном евклидовом кольце. Теоремы о кольцах главных идеалов и о существовании единицы в евклидовом кольце. Разбираются примеры факториальных и нефакториальных колец из числа целых алгебраических расширений второй степени. Разбираются некоторые задачи на делимость в кольце целых чисел. В том числе решаемые с помощью доказанной факториальности некоторых колец целых алгебраических.										
Тема 2. Методы определения простоты и факторизации и их сложность Доказывается тест на простоту Соловея-Штрассена, формулировки тестов на простоту Миллера-Рабина и его аналога для кольца многочленов над полем.	10	2	-	-	-	-	2	2	6	8

Доказывается корректность работы некоторых тестов на простоту чисел специального вида, основанных на последовательностях Лукаша. Разбирается криптосхема с использованием функций Лукаша. Понятие псевдопростоты. Разбираются алгоритмы построения псевдопростых чисел. Доказывается корректность работы алгоритма Берлекэмпа.										
Тема 3. Реализация арифметических операций на компьютере Разбираются быстрые (субквадратичные) версии алгоритма Евклида, алгоритмы модульного умножения и обращения. Их параллельные версии. Доказывается корректность работы и оценки сложности для алгоритмов Карацубы, Шёнхаге (умножения матриц), обращения матриц. Вводится понятие дискретного преобразования Фурье, доказываются теоремы о свертках и доказывается корректность и	15	8	-	-	-	1	9	6	-	6

оценивается вычислительная сложность алгоритма умножения чисел Шёнхаге-Штрассена.										
Тема 4. Асимметричные протоколы. Вводится понятие открытого распределения ключа, аутентификации, цифровой подписи, интерактивности протоколов, нулевого разглашения. Разбирается протокол Сидельникова для открытого распределения ключа. Доказывается его нестойкость в кольце матриц. Разбирается BBS генератор и протокол с числами Блюма. Протоколы аутентификации Антверпена и Шаума. Вводится понятие слепой подписи, достоверной подписи, стираемой подписи, законной стираемой подписи. Разбираются протоколы Шаума, Антверпена, электронные деньги. Разбирается протокол Имаи-Матсумото-Патарина.	9	4	-	-	-	1	5	4	-	4

Тема 5. Методы дискретного логарифмирования Разбираются с оценкой сложности алгоритмы Гедьфонда, Похлига-Хеллмэна, ро и лямбда метод Полларда. Рассматривается параллельные модификации лямбда метода Полларда.	12	7	-	-	-	-	7	6	-	6
6. Промежуточная аттестация – устный экзамен	38	2						36		
Итого	108	40						68		

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

.

Тема 1 «Алгебраические основы теории делимости»
Тема 2 «Методы определения простоты и факторизации и их сложность»
Тема 3 «Реализация арифметических операций на компьютере»
Тема 4 «Асимметричные протоколы»
Тема 5 «Методы дискретного логарифмирования»

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. **Черепнев М.А. Криптографические протоколы: Учебное пособие. – Центр прикладных исследований при механико-математиуеском факультете, 2006.**
2. **Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: МЦНМО, 2003**

Дополнительная литература

1. Б.Л. ванн дер Варден Алгебра М: Наука 1976

   Лиддл, Нидеррейтер Конечные поля т.1 М: Мир 1988

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru
2. www.scopus.com

Информационные технологии, используемые в процессе обучения

1. Программное обеспечение для подготовки слайдов лекций MS PowerPoint

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия
1	Лекция 5	Лекция-конференция на тему «Алгебраические методы в криптографии»
2	Лекция 8	Коллоквиум «Криптопротоколы»

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской и проектором.
Для демонстрации аппаратных средств защиты требуется наличие компьютеров с разъёмом PCI-express.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

доцент, д.ф.-м.н. Черепнев Михаил Алексеевич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Криптосистемы с открытым ключом»

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	**Неудовлетвори-тельно**	**Удовлетвори-тельно**	**Хорошо**	**Отлично**	
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности З1 (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	Отсутствие умений	Фрагментарные умения обоснования степени соответствия	В целом успешное, но не систематическое	Успешное, но содержащее отдельные	Сформированное умение обоснования степени соответствия	Контрольные работы

защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)		защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	пробелы умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	защищаемых объектов информатизации 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	Отсутствие умений	Фрагментарные умения применять	В целом успешное, но не	Успешное, но содержащее	Сформированное умение применять	Контрольные работы

современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения У1 (ПК-1)		современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	систематическое умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	отдельные пробелы умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и 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	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных	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

			разработки и реализации алгоритмов их решения	методов разработки и реализации алгоритмов их решения		
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 компьютерных сетей последнего поколения	Сформированные, но содержащие отдельные пробелы знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированные систематические знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
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	Сформированное умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен

				поколения		
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 области обеспечения информационной безопасности З1(ОПК-1)	Отсутствие знаний	Фрагментарные представления о научных задачах в области обеспечения информационной безопасности	В целом сформированные, но неполные знания о научных задачах в области обеспечения информационной безопасности	Сформированные, но содержащие отдельные пробелы о научных задачах в области обеспечения информационной безопасности	Сформированные систематические знания о научных задачах в области обеспечения информационной безопасности	Устный экзамен
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Устный экзамен

научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)		научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	научных исследований, внедрять полученные результаты в практическую деятельность	
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: содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда. З1(УК-5(6))	Не имеет базовых знаний о сущности процесса целеполагания, его особенностях и способах реализации.	Допускает существенные ошибки при раскрытии содержания процесса целеполагания, его особенностей и способов реализации.	Демонстрирует частичные знания содержания процесса целеполагания, некоторых особенностей профессионального развития и самореализации личности, указывает способы реализации, но не может обосновать	Демонстрирует знания сущности процесса целеполагания, отдельных особенностей процесса и способов его реализации, характеристик профессионального развития личности, но не выделяет критерии выбора	Раскрывает полное содержание процесса целеполагания, всех его особенностей, аргументированно обосновывает критерии выбора способов профессиональной и личностной целереализации при решении профессиональных задач.	Отчеты, доклады на научных семинарах

			возможность их использования в конкретных ситуациях.	способов целереализации при решении профессиональных задач.		
УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей. У1(УК-5(6))	Не умеет и не готов формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.	Имея базовые представления о тенденциях развития профессиональной деятельности и этапах профессионального роста, не способен сформулировать цели профессионального и личностного развития.	При формулировке целей профессионального и личностного развития не учитывает тенденции развития сферы профессиональной деятельности и индивидуально-личностные особенности.	Формулирует цели личностного и профессионального развития, исходя из тенденций развития сферы профессиональной деятельности и индивидуально-личностных особенностей, но не полностью учитывает возможные этапы профессиональной социализации.	Готов и умеет формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.	Отчеты, доклады на научных семинарах
УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений У2 (УК-1)	Отсутствие умений	Частично освоенное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но не систематически осуществляемое умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализаци и исходя из	В целом успешное, но содержащее отдельные пробелы умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализаци и исходя из	Сформированное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	доклады на научных семинарах

			наличных ресурсов и ограничений	наличных ресурсов и ограничений		
ВЛАДЕТЬ: навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач, в том числе в междисциплинарных областях В2 (УК-1)	Отсутствие навыков	Фрагментарное применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но не систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но содержащее отдельные пробелы применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	Успешное и систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	доклады на научных семинарах

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. Понятие евклидового кольца, простого элемента в произвольном кольце, единиц и ассоциированных элементов, факториального кольца. Расширенный алгоритм Евклида.
2. Теоремы об однозначности разложения на простые множители в произвольном евклидовом кольце. Теоремы о кольцах главных идеалов и о существовании единицы в евклидовом кольце. Примеры факториальных и нефакториальных колец из числа целых алгебраических расширений второй степени.

3. Некоторые задачи на делимость в кольце целых чисел. В том числе решаемые с помощью факториальности некоторых колец целых алгебраических.
4. Доказательство теста на простоту Соловея-Штрассена, формулировки тестов на простоту Миллера-Рабина и его аналога для кольца многочленов над полем.
5. Доказательство корректности работы некоторых тестов на простоту чисел специального вида, основанных на последовательностях Лукаша.
6. Криптосхема с использованием функций Лукаша.
7. Понятие псевдопростоты. Алгоритмы построения псевдопростых чисел.
8. Алгоритм Берлекэмпа.
9. Субквадратичные версии алгоритма Евклида, алгоритмы модульного умножения и обращения. Их параллельные версии.
10. Доказательство корректности работы и оценки сложности для алгоритмов Карацубы, Шёнхаге (умножения матриц), обращения матриц.
11. Понятие дискретного преобразования Фурье, теоремы о свертках.
12. Алгоритм умножения чисел Шёнхаге-Штрассена.
13. Понятие открытого распределения ключа, аутентификации, цифровой подписи, интерактивности протоколов, нулевого разглашения.
14. Протокол Сидельникова для открытого распределения ключа. Его нестойкость в кольце матриц.
15. BBS генератор и протокол с числами Блюма. Протоколы аутентификации Антверпена и Шаума.
16. Понятие слепой подписи, достоверной подписи. Протоколы Шаума, Антверпена.
17. Понятие стираемой подписи, законной стираемой подписи. Протокол Шаума.
18. Электронные деньги.
19. Протокол Имаи-Матсумото-Патарина.
20. Алгоритмы Гедьфонда, Похлига-Хеллмэна, ро метод Полларда.
21. Лямбда метод Полларда. Параллельные модификации лямбда метода Полларда.

Материалы для мероприятий текущего контроля.

Мероприятия текущего контроля реализуются в виде тестов с выбором вариантов ответа. Четыре набора тестов охватывают теоретический материал, относящийся соответственно к темам 1, 3, 4 и 5. Вопросы тестов соответствуют приведенным выше вопросам к устному экзамену, раскрывая их на более подробном уровне.

Примерные темы рефератов.

Реферат посвящен Теме 2. Примеры тем:

1. Методические подходы к оценке эффективности защиты речевой информации.
2. Электромагнитные низкочастотные каналы утечки информации.
3. Маскирование сигналов шумами, коррелированными с сигналами.
4. Задачи контроля каналов утечки информации в реальном масштабе времени.

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 каждую контрольную работу и реферат выставляются баллы (максимум 10 баллов за каждый вид работы). Пусть М – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку О1 следующим образом:

меньше М/2 баллов: О1=2;

больше или равно М/2 баллов, но меньше 2М/3: О1=3;

больше или равно 2М/3 баллов, но меньше 5М/6: О1=4;

больше или равно 5М/6 баллов: О1=5.

На экзамене оценка О1 является стартовой. Окончательная оценка определяется исходя из оценки устного ответа студента, при этом она не может отличаться от стартовой оценки более чем на 1 балл.

Структура и график контрольных мероприятий

Контрольная работа на 3-й, 8-й, 10-й, 14-й неделях, реферат в течение семестра, устный экзамен в конце семестра.