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

«Симметричные криптосистемы»

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

Симметричные криптосистемы

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
1. Способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. (ОПК -2)	В1(ОПК-2) Владеть навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. З1 (ОПК-2) Знать Методы исследования решения конкретных исследовательских задач в области обеспечения информационной безопасности. У1(ОПК-2) Уметь разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения

	конкретных исследовательских задач в области обеспечения информационной безопасности.
2. Способность обосновать степень соответствия защищаемых объектов информатизации и информатизационных 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.
3. 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)	У1(УК-1) УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов В1(УК-1) ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях
4. Способность планировать и решать задачи собственного профессионального и личностного развития (УК-5(6))	З1(УК-5(6)) 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. 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.

5. 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 построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения 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

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 операционным системам, компьютерным сетям, базам данных, 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 визуализации выходных последовательностей псевдослучайных генераторов Vorg-5, программное средство визуализации графиков функций Grapher, программное средство просмотра pdf-фалов Adobe Reader.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные проблемы и задачи, связанные с разработкой и анализом симметричных шифров. Основное внимание уделено программно-реализуемым шифрам потокового типа, строению основных блоков и узлов таких шифров, методам синтеза и анализа соответствующих криптографических примитивов, математической теории, на которой основаны данные методы.

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. Основные понятия теории симметричных криптосистем Шифры замены и перестановки. Блоковые и потоковые шифры. Понятие о стойкости и методах дешифрования симметричных		7	-	-	-		7	6	-	6

шифров. Принцип Керкгоффса. Совершенные по Шеннону шифры. Шифры гаммирования и колонной замены. Совершенные шифры, не размножающие ошибку: теорема Котельникова. Эндоморфные шифры. Таблица зашифрования эндоморфного шифра как латинский квадрат. Имитостойкость, вероятность навязывания. Применение ортогональных латинских квадратов для уменьшения вероятности навязывания.										
Тема 2. Криптопримитивы программно-реализуемых потоковых шифров. Основные узлы и блоки современных программно-реализуемых потоковых шифров. Генераторы исходных последовательностей, функции усложнения, фильтры, мультиперестановки. Основные требования к узлам и блокам потоковых шифров. Равновероятность, биективность, транзитивность. Т-функции как структурные элементы криптопримитивов.	10	2	-	-	-	-	2	2	6	8
Тема 3. Математическая теория Т-функций.	15	8	-	-	-	1	9	6	-	6

Т-функции как детерминированные функции на бесконечных бинарных словах. Бесконечные бинарные слова как 2-адические целые числа. Т-функции как 1-липшицевы функции на кольце целых 2-адических чисел. Элементы 2-адического анализа и 2-адической эргодической теории. Равновероятность, биективность, транзитивность Т-функций как сохранение меры и эргодичность.										
Тема 4. Криптографические свойства Т-функций. Критерии и достаточные условия равновероятности/транзитивности (сохранения меры/эргодичности) для Т-функций. Координатные последовательности, линейная сложность, 2-адическая сложность, периоды, зависимости. Статистические свойства Т-функций. Закон 0 или 1 для Т-функций.	9	4	-	-	-	1	5	4	-	4
Тема 5. Методы построения алгоритмов потокового шифрования на основе Т-функций. Построение латинских квадратов и пар ортогональных латинских квадратов на основе Т-функций. Сплетения детерминированных функций и генераторы с	23	12	-	2	-	1	15	8	-	8

динамически изменяющимся законом рекурсии. Построение потоковых шифров как сплетений Т-функций.										
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 «Основные понятия теории симметричных криптосистем»

- ✓ Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003
- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002

Тема 2 «Криптопримитивы программно-реализуемых потоковых шифров»

- ✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).

Тема 3 «Элементы математической теории Т-функций»

- ✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).
- ✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте http://istina.msu.ru/courses/7102110/).
- ✓ Анашин В.С. Введение в прикладной p-адический анализ. - М.: 2008 (электронная версия http://istina.msu.ru/courses/7102110/).
- ✓ Коблиц Н. p-адические числа, p-адический анализ и дзета-функции. - М.: Мир, 1982
- ✓ Хренников А.Ю. Неархимедов анализ и его приложения. – М.: Физматлит, 2003

✓ Каток С.Б. p-адический анализ в сравнении с вещественным. –М.: МЦНМО, 2004
✓ Кнут Д. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. - Москва–СПб–Киев: Вильямс, 2000
✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y.,2009.
✓ Anashin V. The p-adic ergodic theory and applications (электронная версия https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications)

Тема 4 «Криптографические свойства Т-функций»

✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).
✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте http://istina.msu.ru/courses/7102110/).
✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y.,2009.
✓ Anashin V. The p-adic ergodic theory and applications (электронная версия https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications)

Тема 5 «Методы построения алгоритмов потокового шифрования на основе Т-функций»

✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
✓ Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).
✓ Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте http://istina.msu.ru/courses/7102110/).
✓ Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003
✓ Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y.,2009.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
3. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002
4. Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003

5. Анашин В.С. Неархимедов анализ, Т-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).
6. Анашин В.С. Методы неархимедовой алгебраической динамики в криптографии. - М.: 2011 (электронная версия доступна на сайте http://istina.msu.ru/courses/7102110/).
7. Анашин В.С. Введение в прикладной p-адический анализ. - М.: 2008 (электронная версия http://istina.msu.ru/courses/7102110/).

Дополнительная литература

1. Коблиц Н. p-адические числа, p-адический анализ и дзета-функции. - М.: Мир, 1982.
2. Хренников А.Ю. Неархимедов анализ и его приложения. – М.: Физматлит, 2003
3. Каток С.Б. p-адический анализ в сравнении с вещественным. –М.: МЦНМО, 2004
4. Кнут Д. Искусство программирования для ЭВМ. т. 2. Получисленные алгоритмы. - Москва–СПб–Киев: Вильямс, 2000
5. Anashin V., Khrennikov A. Applied Algebraic Dynamics, volume 49 of deGruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin—N.Y.,2009.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. http://istina.msu.ru/courses/7102110/
2. https://www.researchgate.net/profile/Vladimir_Anashin

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 средство визуализации выходных последовательностей псевдослучайных генераторов Vorg-5
4. Программное средство визуализации графиков функций Grapher

Активные и интерактивные формы проведения занятия

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия

1	Лекция 8	Лекция-конференция на тему «Схемы современных шифраторов на основе Т-функций»
2	Лекция 16	Деловая игра «Разработка блок-схемы потокового шифратора на основе сплетений»

Материально-техническая база

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

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

профессор, д.ф.-м.н. Анашин Владимир Сергеевич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Симметричные криптосистемы»

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 защищаемых	Отсутствие умений	Фрагментарные умения обоснования степени соответствия защищаемых	В целом успешное, но не систематическое умение	Успешное, но содержащее отдельные пробелы умение	Сформированное умение обоснования степени соответствия защищаемых	Контрольные работы

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

построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения У1 (ПК-1)		построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	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	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 разработки и	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	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

			реализации алгоритмов их решения	разработки и реализации алгоритмов их решения		
ВЛАДЕТЬ: Навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности В1(ОПК-2)	Отсутствие знаний	Фрагментарное владение навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	В целом успешное, но не полное владение навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Успешное, но содержащее отдельные пробелы навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Сформированное владение навыками навыками разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Контрольные работы, реферат
Знать: Методы исследования решения конкретных исследовательских задач в области обеспечения информационной безопасности. З1(ОПК-2)	Отсутствие знаний	Фрагментарные представления о методах исследования решения конкретных исследовательских задач в области обеспечения информационной безопасности.	В целом сформированные, но неполные знания о методах исследования решения конкретных исследовательских задач в области обеспечения информационной	Сформированные, но содержащие отдельные пробелы знания о методах исследования решения конкретных исследовательских задач в области обеспечения информационной	Сформированные систематические знания о методах исследования решения конкретных исследовательских задач в области обеспечения информационной безопасности.	Устный экзамен

			безопасности.	безопасности.		
Уметь разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности. У1(ОПК-2)	Отсутствие умений	Фрагментарные умения разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	В целом успешное, но не систематическое умение разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	Успешное, но содержащее отдельные пробелы умение разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	Сформированное умения разработки частных методов исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	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 возможность их	Демонстрирует знания сущности процесса целеполагания, отдельных особенностей процесса и способов его реализации, характеристик профессионального развития личности, но не выделяет критерии выбора способов	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

			использования в конкретных ситуациях.	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: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыш и реализации этих вариантов У1 (УК-1)	Отсутствие умений	Частично освоенное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыш и реализации этих вариантов	В целом успешно, но не систематически осуществляемые анализ альтернативных вариантов решения исследовательских и практических задач и оценка потенциальных выигрышей/проигрышей реализации этих	В целом успешно, но содержащие отдельные пробелы анализ альтернативных вариантов решения исследовательских задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов	Сформированное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыш и реализации этих вариантов	доклады на научных семинарах

			вариантов			
ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях В1 (УК-1)	Отсутствие навыков	Фрагментарное применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	В целом успешное, но не систематическое применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	В целом успешное, но содержащее отдельные пробелы применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	Успешное и систематическое применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях	доклады на научных семинарах

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. Общее определения шифра, симметричного шифра и асимметричного шифра. Типы симметричных шифров. Блоковые и потоковые шифры. Шифры гаммирования и колонной замены. Совершенные шифры. Примеры совершенных шифров.
2. Совершенные шифры, не размножающие ошибку. Эндоморфные шифры. Таблица зашифрования эндоморфного шифра. Имитостойкость эндоморфного шифра и методы ее обеспечения.
3. Основные узлы и блоки современных программно-реализуемых потоковых шифров. Генераторы исходных последовательностей, функции усложнения, фильтры, мультиперестановки. Основные требования к узлам и блокам потоковых шифров. Генератор гаммы наложения как автомат. Периодичность гаммы. Равновероятность, биективность, транзитивность детерминированных функций.
4. Детерминированные функции бинарных автоматов как 1-липшицевы функции пространства целых 2-адических чисел. Необходимое и достаточное условие детерминированности 2-адической функции.
5. Определение Т-функции. Базисные команды процессора, являющиеся Т-функциями. Тождества.
6. Кольцо целых 2-адических чисел. Каноническая форма представления целого 2-адического числа. 2-адическая метрика и ее свойства. Шары и треугольники в пространстве целых 2-адических чисел.
7. Арифметика кольца целых 2-адических чисел. Обратимые элементы. Рациональные числа в кольце целых 2-адических чисел.
8. Предел и сходимость в кольце целых 2-адических чисел. Критерий сходимости рядов в этом кольце.
9. Непрерывные функции на кольце целых 2-адических чисел. Непрерывность Т-функций.

10. Представление Т-функций в координатной форме, в виде ряда Малера, в виде ряда ван дер Пута.
11. Дифференцируемые функции на кольце целых 2-адических чисел. Производные команд процессора.
12. Вероятностная мера на кольце целых 2-адических чисел. Функции, сохраняющие меру и эргодические функции. Изометричность сохраняющих меру Т-функций.
13. Основная эргодическая теорема для Т-функций. Сохранение меры и биективность (равновероятность), эргодичность и транзитивность.
14. Критерий сохранения меры/эргодичности для Т-функции в терминах координатных функций.
15. Критерий сохранения меры/эргодичности для Т-функции в терминах рядов Малера и представление сохраняющих меру/эргодических Т-функций.
16. Критерий сохранения меры/эргодичности для Т-функции в терминах рядов ван дер Пута.
17. Критерий и достаточные условия сохранения меры для Т-функции нескольких переменных.
18. Построение латинских квадратов и пар взаимно-ортогональных латинских квадратов с помощью как сохраняющих меру Т-функций.
19. Сохранение меры/эргодичность дифференцируемых Т-функций.
20. Строение координатных последовательностей эргодических Т-функций. Линейная сложность (над полем из 2-х элементов) координатной последовательности эргодической Т-функции.
21. Линейная сложность последовательности, порожденной эргодической Т-функцией, над кольцом целых 2-адических чисел.
22. Графики Т-функций на действительной плоскости. Закон 0 или 1 для Т-функций.
23. Сплетения детерминированных функций. Теорема о строении последовательности, порожденной сплетением детерминированной функции и эргодической Т-функции.
24. Сплетения детерминированных функций. Теорема о распределении n-грамм в последовательности, порожденной сплетением детерминированной функции и эргодической Т-функции.
25. Построение генераторов с динамически изменяющимся законом рекурсии, имеющих максимально возможный период по каждой координатной последовательности, с помощью сплетений.
26. Линейная сложность координатных последовательностей генераторов с изменяющимся законом рекурсии, построенных с помощью сплетений.

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. Потоковые шифры серии TF
2. Потоковые шифры серии TSC
3. Потоковый шифр ASC

4. Потоковый шифр ABC
5. Потоковый шифр VEST
6. Потоковый шифр Mir-1
7. Потоковый шифр Rabbit
8. Потоковый шифр HC-128
9. Потоковый шифр Salsa 20/12
10. Потоковый шифр SOSEMANUK

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.