МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

«Утверждаю»

Декан факультета ВМК МГУ
имени М.В. Ломоносова

академик _____ И.А. Соколов

«___»_____ 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Поточные шифры на основе Т-функций»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки – 10.06.01 «Информационная безопасность»

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

2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Поточные шифры на основе Т-функций

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

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

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к специальным дисциплинам вариативной части образовательной программы и является обязательной для освоения в 4-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

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». Кроме того, учащиеся должны владеть знаниями по симметричным криптосистемам в объеме курса «Симметричные криптосистемы» по профилю «Методы и системы защиты информации, информационная безопасность» (05.13.19).

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 поточных шифров на основе T-функций. Основное внимание уделено программно-реализуемым шифрам этого типа, строению основных блоков и узлов этих шифров, их криптографическим свойствам, методам синтеза и анализа соответствующих криптографических примитивов, а также p-адической эргодической 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 p-адической эргодической теории Пространство целых p-адических чисел как метрическое пространство и пространство с вероятностной мерой Хаара. Функции, сохраняющие меру; эргодические функции. Детерминированные функции как функции, удовлетворяющие p-адическому условию Липшица с константой 1 (1-липшицевы функции). T-функции			-	-	-		7	6	-	6

как 1-лишицевы 2-адические функции. Основная теорема р-адической эргодической теории для детерминированных функций. Признаки и критерии сохранения меры/эргодичности для детерминированных функций.										
Тема 2. Основные блоки и узлы программно-реализуемых потоковых шифров на основе Т-функций. Генераторы исходных последовательностей на основе эргодических Т-функций. Детерминированные функции, эргодические на подпространствах (шарах, сферах) и основанные на них генераторы. Функции усложнения, фильтры на Т-функциях, сохраняющих меру. Мультиплексоры на основе детерминированных 1-липшицевых функций.	10	2	-	-	-	-	2	2	6	8
Тема 3. Криптографические характеристики криптопримитивов, основанных на Т-функциях. Строение координатных последовательностей генераторов, основанных на эргодических Т-функциях, теорема о реализации любых полупериодов. Линейная сложность координатных последовательностей эргодических Т-функций. Линейные зависимости между соседними координатными последовательностями равномер-	15	8	-	-	-	1	9	6	-	6

но-дифференцируемых Т-функций. Графики Т-функций в евклидовом пространстве, теорема о линейности гладких кривых на графиках Т-функций: соответствующих конечным автоматам. Критерий конечной детерминированности Т-функции. Неравномерность длин периодов координатных последовательностей .генераторов: основанных на Т-функциях. Методы увеличения длин периодов младших координатных последовательностей: перестановка разрядов и сплетение детерминированных функций. Основные криптографические свойства координатных последовательностей сплетений Т-функций.										
Тема 4. Статистические свойства поточных шифров на основе Т-функций. Полная и абсолютная транзитивность. Закон 0 или 1 для Т-функций. Теорема о том, что конечно-детерминированные функции имеют меру 0. Методы построения Т-функций полной меры. Многомерные распределения, равномерность распределений выходных последовательностей нелинейных полиномиальных генераторов. Синхронизируемость функции усложнения как достаточное условие равномерности распределения усложненной последоваетльности.	9	4	-	-	-	1	5	4	-	4
Тема 5. Шифраторы с	23	12	-	2	-	1	15	8	-	8

динамически изменяющимся законом шифрования на основе Т-функций. Примеры существующих шифраторов на основе Т-функций, их достоинства и недостатки. Шифраторы с динамически изменяющимся законом шифрования как сплетения автоматов. Основные свойства сплетений. Теорема о строении выходной последовательности сплетения автоматов. Усеченные Т-функции как сплетения. Сплетения Т-функций с другими функциями. Построение неклонируемых шифраторов на основе 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 р-адической эргодической теории»

- ✓ 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 2 «Основные блоки и узлы программно-реализуемых потоковых шифров на основе T-функций»

✓ 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, T-функции и криптография.- М.: 2007 (электронная версия http://istina.msu.ru/courses/7102110/).
✓ 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 3 «Криптографические характеристики криптопримитивов, основанных на T-функциях.»

✓ 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, T-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/).
✓ 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 «Статистические свойства поточных шифров на основе 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
- ✓ Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001
- ✓ 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 «Шифраторы с динамически изменяющимся законом 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.
- ✓ Anashin V. The p-adic ergodic theory and applications (электронная версия https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications)

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/).
8. Anashin V. The p-adic ergodic theory and applications (электронная версия https://www.researchgate.net/publication/269571423_The_p-adic_ergodic_theory_and_applications)

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 «Атаки на современные поточные шифраторы на основе Т-функций»
2	Лекция 16	Деловая игра «Разработка блок-схемы неклонируемого потокового шифратора на основе сплетений Т-функций »

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	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**	
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности 31 (ОПК-3)	Отсутствие знаний	Фрагментарные представления о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	В целом сформированные, но неполные знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные систематические знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Устный экзамен
УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и	Отсутствие умений	Фрагментарные умения обоснования степени соответствия защищаемых объектов информатизации	В целом успешное, но не систематическое умение обоснования степени соответ-	Успешное, но содержащее отдельные пробелы умение обоснования степени соответ-	Сформированное умение обоснования степени соответствия защищаемых объектов информатизации	Контрольные работы

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

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

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

З1(ОПК-1)		безопасности	чения информационной безопасности	обеспечения информационной безопасности	мационной безопасности	
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Устный экзамен
ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность В1(ОПК-1)	Отсутствие навыков	Фрагментарное владение навыками внедрения полученных результатов в практическую деятельность	В целом успешное, но не полное владение навыками внедрения полученных результатов в практическую деятельность	Успешное, но содержащее отдельные пробелы владение навыками внедрения полученных результатов в практическую деятельность	Сформированное владение навыками внедрения полученных результатов в практическую деятельность	устный экзамен

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. 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.
2. Детерминированные функции бинарных автоматов как 1-липшицевы функции пространства целых 2-адических чисел. Необходимое и достаточное условие детерминированности 2-адической функции.
3. Определение T-функции. Базисные команды процессора, являющиеся T-функциями. Тождества.
4. 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.
5. Арифметика кольца целых 2-адических чисел. Обратимые элементы. Рациональные числа в кольце целых 2-адических чисел.
6. Предел и сходимость в кольце целых 2-адических чисел. Критерий сходимости рядов в этом кольце.
7. Непрерывные функции на кольце целых 2-адических чисел. Непрерывность T-функций.
8. Представление T-функций в координатной форме, в виде ряда Малера, в виде ряда ван дер Пута.
9. Дифференцируемые функции на кольце целых 2-адических чисел. Производные команд процессора.
10. Вероятностная мера на кольце целых 2-адических чисел. Функции, сохраняющие меру и эргодические функции. Изометричность сохраняющих меру T-функций.
11. Основная эргодическая теорема для T-функций. Сохранение меры и биективность (равновероятность), эргодичность и транзитивность.
12. Критерий сохранения меры/эргодичности для T-функции в терминах координатных функций.
13. Критерий сохранения меры/эргодичности для T-функции в терминах рядов Малера и представление сохраняющих меру/эргодических T-функций.
14. Критерий сохранения меры/эргодичности для T-функции в терминах рядов ван дер Пута.
15. Критерий и достаточные условия сохранения меры для T-функции нескольких переменных.
16. Построение латинских квадратов и пар взаимно-ортогональных латинских квадратов с помощью сохраняющих меру T-функций.
17. Классы A,B,C T-функций.
18. Сохранение меры/эргодичность дифференцируемых T-функций.
19. T-функции, эргодические на подпространствах. Критерии эргодичности T-функций на шарах и сферах.
20. Эргодичность T-функций, в композицию которых входит операция взятия обобщенного обратного.
21. Строение координатных последовательностей эргодических T-функций. Линейная сложность (над полем из 2-х элементов) координатной последовательности эргодической T-функции.
22. Линейные зависимости между координатными последовательностями равномерно-дифференцируемых T-функций.
23. Линейная сложность последовательности, порожденной эргодической T-функцией, над кольцом целых 2-адических чисел и полем 2-адических чисел; 2-адическая сложность.
24. Теорема о существовании T-функции с заданным набором полупериодов координатных последовательностей.

25. Теорема о периодах и линейной сложности координатных последовательностей, усложненных с помощью функции перестановки разрядов и эргодической Т-функции.
26. Графики Т-функций в евклидовом пространстве. Закон 0 или 1 для Т-функций. Теорема о том, что детерминированная функция конечного автомата имеет нулевую меру.
27. Критерий конечной детерминированности Т-функции в терминах рядов ван дер Пута.
28. Полная и абсолютная транзитивность. Связь с мерой Т-функции. Методы построения Т-функций, имеющих меру 1.
29. Распределения n-грамм в последовательностях, порожденных эргодическими Т-функциями.
30. Сплетения детерминированных функций. Теорема о строении последовательности, порожденной сплетением детерминированной функции и эргодической Т-функции.
31. Теорема о распределении n-грамм в последовательности, порожденной сплетением детерминированной функции и эргодической Т-функции.
32. Построение генераторов с динамически изменяющимся законом рекурсии, имеющих максимально возможный период по каждой координатной последовательности, с помощью сплетений.
33. Линейная сложность координатных последовательностей генераторов с изменяющимся законом рекурсии, построенных с помощью сплетений
34. Теорема о существовании сплетения с заданным набором полупериодов координатных последовательностей.
35. Понятие о физически неклонируемых функциях. Использование ПЛИС для создания физически неклонируемых шифраторов на основе Т-функций. «Неклонируемый параметр». Классы эргодических Т-функций с «неклонируемым параметром» (примеры, формулировки теорем).

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. Системы ортогональных Т-функций.
2. Эргодические алгебраические Т-функции на сферах.
3. Различные критерии сохранения меры для детерминированных функций.
4. Ограниченная детерминированность Т-функций и ее связь с таблицами истинности.
5. Эргодические Т-функции с возмущениями.
6. Неклонируемые криптопримитвы на ПЛИС.
7. Обобщения Т-функций и крптопримитивы на них.
8. Вопросы сложности реализации Т-функций.
9. Физически неклонируемые функции: обзор известных методов.
10. Строго липшицевы Т-функции.

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 M – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку O1 следующим образом:

меньше M/2 баллов: O1=2;

больше или равно M/2 баллов, но меньше 2M/3: O1=3;

больше или равно 2M/3 баллов, но меньше 5M/6: O1=4;

больше или равно 5M/6 баллов: O1=5.

На экзамене оценка O1 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.