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

«Дискретные функции в символической динамике»

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

Дискретные функции в символической динамике

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 в 3-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения

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
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 формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1)	З1(ОПК-1) ЗНАТЬ 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

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.
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.

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

36 часов составляет контактная работа с преподавателем – 34 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часа мероприятий текущего контроля успеваемости, 0 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

72 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по алгебре, 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» и/или 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные понятия символической динамики и развивается атематический аппарат, использующий результаты алгебры, комбинаторики, теории графов и тории автоматов. Анализируются связи основных понятий символической динамики с некоторыми криптографическими примитивами и классами линейных кодов, исправляющими ошибки. Приводятся примеры сведения криптографических и теоретико-кодовых задач к задачам символической динамики.

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. Введение в теорию динамических систем Метрические пространства. Нормы и метрики. Примеры метрических пространств.Сходимость последовательностей и непрерывность отображений.Открытые и замкнутые множества.Понятие компактности пространства. Критерий компактности множества в компактном пространстве. Теорема Больцано . Критерий компактности множества в метрическом пространстве(теорема Гейне-Бореля). Плотность множеств. Теорема Бэра. Определение динамической системы Примеры. Инварианты динамических систем. Дзета-функция. Марковские разбиения.	8	8	-	-	-		8	-	-	-

Тема 2 Сдвиговые пространства(сдвиги) как фазовые пространства в символической динамике. Основные понятия и термины.Полный сдвиг над конечным алфавитом. Примеры. Трансляция и коммутирующие с ней отображения. Понятие сдвигового пространства (сдвига).Блоки(слова) — запреты. Примеры. Языки, порождаемые сдвигами. Необходимые и достаточные условия принадлежности слова языку, порожденному сдвигом. Сдвиги, порождаемые операциями «расширение» и «расширение с зацеплением». Некоторые свойства и параметры порождаемых сдвиговых пространств	8	8	-	-	-	-	8	-	-	-

Тема 3. Скользящие блочные коды. Понятие скользящего блочного кода. Примеры. Простейшие свойства скользящих блочных кодов. Теорема о «гомоморфизме» для скользящего блочного кода. Понятие сопряженности. Теретико — кодовые модели скользящих блочных кодов. Сверточные коды, исправляющие ошибки. Криптографические модели скользящих блочных кодов. Регистры сдвига с фильтрующими функциями. Фильтрующие и комбинирующие генераторы..	6	6	-	-	-	-	6	-	-	-

Тема 4. Сдвиговые пространства конечного типа. Понятие сдвига конечного типа. Примеры. Сдвиги конечного типа с памятью. Теорема о совпадении класса сдвигов конечного типа с классом сдвигов конечного типа с памятью. Критерий для сдвигов конечного типа с памятью. Теорема о сопряженности с о сдвигом конечного типа Графы и порождаемые ими сдвиги. Примеры. Простейшие свойства сдвигов, порожденных графами. Теоретико-графовое представление сдвигов конечного типа с памятью Софические сдвиги и их простейшие свойства. Понятие энтропии сдвига. Вычисление энтропии.	6	6	-	-	-	-	6	-	-	-

Тема 5. Использование методов символической ддинамики для реализации атак на фильтрующие генераторы. Сдвиги, порождаемые линейными рекуррентами над конечными полями, и их основные свойства. Фильтрующие функции и их параметры. Использование теоремы о сопряженности для сведения криптографических задачи к задачам символической динамики. Новые криптографические параметры фильтрующих генераторов и их влияние на эффективность решения криптографических задач. Примеры	6	6	-	-	-		6	-	-	-
6. Промежуточная аттестация – устный экзамен	74	2						72		
Итого	108	36						72		

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 **« Введение в теорию динамических систем»**
Тема 2 «Сдвиговые пространства(сдвиги) как фазовые пространства в символической динамике»
Тема 3 «Скользящие блочные коды»
Тема 4 «Сдвиговые пространства конечного типа»
Тема 5 «Использование методов символической ддинамики для реализации атак на фильтрующие генераторы»

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

D.Lind, B.Marcus. An Introduction tj Symbolic Dynamics and Coding. Cambridge University Press 1995, pp. 495.

Ресурсы информационно-телекоммуникационной сети «Интернет»

http://cryptography.ru
www.iacr.org

Материально-техническая база

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

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

доцент, к.ф.-м.н. Логачев Олег Алексеевич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Дискретные функции в символической динамике»

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

ЗНАТЬ: 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 реализации алгоритмов их решения У1 (ПК-1)	Отсутствие умений	Фрагментарные умения применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	В целом успешное, но не 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	Успешное, но содержащее 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	Сформированное умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	Устный экзамен

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

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 использования в конкретных ситуациях.	Демонстрирует знания сущности процесса целеполагания, отдельных особенностей процесса и способов его реализации, характеристик профессионального развития личности, но не выделяет критерии выбора способов целереализации при решении профессиональных задач.	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
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

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. Метрические пространства, норма и метрика. Примеры.
2. Понятие сходимости в метрическом пространстве.
3. Понятие открытого и замкнутого множеств.
4. Компактность пространств и множеств: характеризация с помощью последовательностей.
5. Компактность пространств и множеств: характеризация с помощью открытых множеств.
6. Теорема Больцано-Вейерштрасса.
7. Теорема Гейне-Бореля.
8. Теорема Бэра.
9. Понятие динамической системы. Примеры.
10. Инварианты динамической системы. Примеры.
11. Дзета-функция динамической системы. Примеры вычисления дзета-функций для некоторых классов динамических систем.
12. Марковские рахбиения и символьное представления динамических систем.
13. Сдвиговые пространства(сдвиги) над конечным алфавитом.Полный сдвиг и другие примеры.
14. Характеризация сдвиговых пространств через множества запретов. Примеры.
15. Языки, порождаемые сдвигами. Критерии принадлежности слова языку. Неприводимые сдвиги.
16. Операция «расширения» сдвига и ее свойства.
17. Операция «расширения с зацеплением» сдвига и ее свойства.
18. Понятие скользящего блочного кода и его основные параметры. Примеры.
19. Понятие сопряженности сдвигов. Примеры.
20. Теорема о «гомоморфизме» для скользящего блочного кода.
21. Сверточные линейные коды. Примеры.
22. Сдвиги конечного типа.Примеры.
23. Сдвиги конечного типа с памятью. Примеры.
24. Критерий для сдвига конечного типа с памятью.
25. Теорема о свойствах сдвига сопряженного со сдвигом конечного типа.
26. Сдвиги, порождаемые конечными грфами, и их матричное описание. Примеры.
27. Теоретико-графовые представления сдвигов конечного типа. Теорема о представлении сдвига конечного типа с памятью графом.
28. Комбинирующий генератор, его основные параметры и свойства.
29. Фильтрующий генератор, его основные параметры и свойства.

30. Атаки на фильтрующий и комбинирующий генератор сизвестным открытым текстом. Методы реализации угроз.
31. Использование математических моделей символической динамики для описания комбинирующего генератора.
32. Использование математических моделей символической динамики для описания фильтрующего генератора.
33. Использование сопряженности для построения обратных отображений для скользящих блочных кодов, описывающих комбинирующие и фильтрующие генераторы.
34. Понятие энтропии сдвигового пространства и ее основные свойства.
35. Примеры вычисления энтропии для некоторых классов сдвигов..

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятием прочитать конспект предыдущей лекции. После каждого занятия рекомендуется прочитать дополнительную литературу по теме лекции и привести в порядок свои конспекты.

Система контроля и оценивания

В каждом билете содержится 2 вопроса из приведенного в ФОС списка – 1-й на темы 1,2, а 2-й – на темы 3-5.

Структура и график контрольных мероприятий

Контрольные мероприятия в течение семестра отсутствуют.