Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

УТВЕРЖДАЮ
Декан факультета ВМК МГУ
Академик _____ /*И.А. Соколов*/
«14» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дискретные функции в символической динамике
Discrete functions in symbolic dynamics

Программа (программы) подготовки научных и научно-педагогических кадров в аспирантуре

102.01.00.112-фмн-кфап, 102.01.00.122-фмн-кмф, 102.01.00.122-фмн- кски,
102.01.00.235-фмн- кски, 102.01.00.112-фмн-ком, 102.01.00.122-фмн-кани
102.01.00.112-фмн-кса, 102.01.00.122-фмн- кса, 102.01.00.112-фмн- кндсипу,
102.01.00.122-фмн- кндсипу, 102.01.00.114-фмн- кмс, 102.01.00.115-фмн- кммп
102.01.00.115-фмн- кмк, 102.01.00.123-фмн- кмк, 102.01.00.116-фмн- квтм,
102.01.00.122-фмн- квтм, 102.01.00.116-фмн- квм, 102.01.00.122-фмн- квм, 102.01.00.122-фмн- коу,
102.01.00.112-фмн- коу, 102.01.00.123-фмн- кио, 102.01.00.122-фмн- кио, 102.01.00.235-фмн- киит,
102.01.00.235-фмн-касвк, 102.01.00.235-фмн- ксп, 102.01.00.235-фмн- киб,
102.01.00.236-фмн-киб, 102.01.00.235-фмн-кая

Москва 2022

Рабочая программа дисциплины разработана в соответствии с Приказом Ректора МГУ №1216 от 24 ноября 2021 года «Об утверждении Требований к основным программам подготовки научных и научно-педагогических кадров в аспирантуре, самостоятельно устанавливаемых Московским государственным университетом имени М.В. Ломоносова»

1. Краткая аннотация:

Название дисциплины Дискретные функции в символической динамике

Цель изучения дисциплины – Данный курс посвящен изучению использования математического аппарата дискретных функций для описания основных понятий символической динамики и их свойств. В курсе используются результаты алгебры, комбинаторики, теории графов, теории кодирования, криптографии и теории автоматов. Анализируются связи основных понятий символической динамики с некоторыми криптографическими примитивами и классами кодов, исправляющих ошибки.

2. Уровень высшего образования –аспирантура

3. Научная специальность 2.3.6 – «Методы и системы защиты информации, информационная безопасность»,область науки**:** физико-математические науки

4. Место дисциплины (модуля) в структуре Программы аспирантуры: элективный курс.

5.Объем дисциплины (модуля) составляет 2 зачетные единицы, всего 108 часов, из которых 34 часа занятий лекционного типа, 72 часа самостоятельной работы аспирантов и 2 часа – экзаменационная аттестация.

6. Входные требования для освоения дисциплины (модуля), предварительные условия.

На предыдущих уровнях высшего образования должны быть освоены общие курсы:

1.Дискретная математика

2.Алгебра

3.Комбинаторика

4. Функциональный анализ

5. Теория кодирования

6. Математическая криптография

7. Содержание дисциплины (модуля), структурированное по темам

Наименование и краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**Всего** **(часы)**	В томчисле								
		Контактная работа (работа во взаимодействии с преподавателем), часы изних						**Самостоятельная работа обучающегося, часы** из них		
		Занятиялекционного типа	Занятиясеминарского типа	Групповыеконсультации	Индивидуальныеконсультации	Учебные занятия, направленные на проведение текущего контроля успеваемости, промежуточной аттестации	**Всего**	Выполнениедомашнихзаданий	Подготовка к коллоквиумам	**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	18	6					6	12	-	12

пространстве. Теорема Больцано. Критерий компактности множества в метрическом пространстве (теорема Гейне-Бореля). Плотность множества. Теорема Бэра. Определение динамической системы. Примеры. Инварианты динамических систем. Дзета-функция. Марковские разбиения.										
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.	20	6					6	14	-	14

Сдвиги, порождаемые операциями «расширение» и «расширение с зацеплением». Некоторые свойства и параметры порождаемых пространств.										
Тема 3. Скользящие блочные коды Понятие скользящего блочного кода. Примеры. Простейшие свойства скользящих блочных кодов. Теорема о «гомоморфизме» для скользящего блочного кода. Понятие сопряженности. Теоретико-кодовые модели скользящих блочных кодов. Сверточные коды, исправляющие ошибки. Криптографические модели скользящих блочных кодов. Регистры сдвига с фильтрующими функциями. Фильтрующие и комбинирующие генераторы.	22	8					8	14	-	14
Тема 4. Сдвиговые пространства конечного типа	24	8					8	16	-	16

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 со 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.										
Тема 5. Использование методов символической динамики Сдвиги, порождаемые линейными рекуррентаминад конечными полями, и их	22	6					6	16		16

основные свойства. Фильтрующие функции и их параметры. Использование теоремыо сопряженности для сведения криптографической задачи к задачам символической динамики. Новые криптографические параметры фильтрующих генераторов и их влияние на эффективность решения криптографических задач. Примеры.										
Промежуточная аттестация: устный экзамен	2									
Итого	108									

8. Образовательные технологии.

При проведении лекционных занятий не предусматривается использование информационных технологий, включающих пакеты математических программ:MATLAB, MATHEMATICA и др.

9. Учебно-методические материалы для самостоятельной работы по дисциплине (модулю):

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»

- ✓ M. Brin., G. Stuck. Introductiontodynamicalsystems. Cambridge University Press, 2003, pp. 240.

Тема 2 «Сдвиговые пространства (сдвиги) как фазовые пространства в символической динамике»

- ✓ D. Lind, B. Marcus. An introduction to symbolic dynamics and coding. Cambridge University Press,1995, pp. 495.

Тема 3 «Скользящие блочные коды»

- ✓ D. Lind, B. Marcus. An introduction to symbolic dynamics and coding. Cambridge University Press,1995, pp. 495.

Тема 4 «Сдвиговые пространства конечного типа»

- ✓ D. Lind, B. Marcus. An introduction to symbolic dynamics and coding. Cambridge University Press,1995, pp. 495.

Тема 5. «Использование методов символической динамики для реализации атак на фильтрующие генераторы»

- ✓ D. Lind, B. Marcus. An introduction to symbolic dynamics and coding. Cambridge University Press,1995, pp. 495.

10. Ресурсноеобеспечение:

- Перечень основной и вспомогательной учебной литературы ко всему курсу

Основная литература:

- ✓ M. Brin., G. Stuck. Introductiontodynamicalsystems. Cambridge University Press, 2003, pp. 240.
- ✓ D. Lind, B. Marcus. An introduction to symbolic dynamics and coding. Cambridge University Press,1995, pp. 495.

Дополнительнаялитература:

1. B.P. Kitchens. Symbolic Dynamics. One-sided, two-sided and countable state Markov shifts. Springer, 1997, pp. 262.
2. G.A. Hedlund. endomorphisms and automorphisms of the shift dynamical system. Math. systemstheory, 3, 1969, pp. 320-375.

.

- Переченьиспользуемыхинформационныхтехнологий, используемыхприосуществлениобразовательногопроцесса, включаяпрограммное обеспечение, информационные справочные системы (при необходимости):

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

- Описаниематериально-техническойбазы.
  Занятия могут проводятся в аудитории, не оснащенной мультимедийным экраном

11. Язык преподавания – русский

12. Преподаватели:

Степень, должность ФИО.,e-mail, тел.: -д.ф.-м.н., доцент Логачев Олег Алексеевич,ollog@inbox.ru ,8(495)930 4386

Фонды оценочных средств, необходимые для оценки результатов обучения

Образцы домашних заданий:

1. Является ли пересечение языков двух сдвигов языком некоторого сдвига?
2. Является ли пересечение двух неприводимых сдвигов неприводимым сдвигом?
3. Доказать, что обратимый скользящий блоковый код имеет только один обратный.
4. Кроме того в качестве домашнего задания подразумевается изучение рекомендуемой литературы.

Вопросы для промежуточной аттестации – **зачета (экзамена)**:

1. Критерий компактности множества в компактном пространстве.
2. Критерий компактности множества в метрическом пространстве.
3. Теорема о необходимых и достаточных условияхпринадлежности слова языку,порожденному сдвигом .
4. Теорема о «гомоморфизме» для скользящего блочного кода.
5. Теорема о совпадении класса сдвигов конечного типа с классом сдвигов конечного типа с памятью.
6. Критерий для сдвига конечного типа.
7. Теорема о существовании графа, порождающего произвольный сдвиг конечного типа с памятью.
8. Теорема о сопряженности со сдвигом конечного типа.
9. Теорема о сопряженности сдвигов конечного типа.
10. Критерий софичности сдвига.

Методические материалы для проведения процедур оценивания результатов обучения

Зачет (экзамен) проходит по билетам, включающем 2 вопроса. Уровень знаний аспиранта по каждому вопросу на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».