Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Криптографические свойства дискретных функций**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по математическому анализу и линейной алгебре в объеме, соответствующем программе первого года обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки» (или отсутствуют).

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-1.Б** Способность применять и адаптировать существующие математические и компьютерные методы для разработки и реализации алгоритмов решения актуальных задач в области фундаментальной и прикладной математики
* **ОПК-2.Б** Способность применять и модифицировать математические модели, а также интерпретировать полученные математические результаты при решения задач в области профессиональной деятельности
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппарат

(Не следует увлекаться количеством компетенций. Если дисциплина относится к вариативной части программы, то она может не развивать никаких ОПК, зато может развивать свои собственные специализированные ПК (СПК), формулировки которых может придумать автор курса. В этом случае *код* компетенции должен выглядеть так: СПК-<аббревиатура названия курса>-<номер СПК для курса>.Б. Например, для курса ОДУ коды могли бы выглядеть так: СПК-ОДУ-1.Б, СПК-ОДУ-2.Б, ...)

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. теоретические основы спектрального метода анализа (Фурье) криптографических булевых функций;
2. теоретические основы алгебраических методов анализа криптографических булевых функций;
3. теоретические основы комбинаторных методов анализа криптографических булевых функций;
4. теоретические основы групповой эквивалентности булевых функций;
5. основы алгебраической и метрической теорий полиномиальных кодов Рида-Маллера;
6. методологию анализа и синтеза максимально-нелинейных булевых функций;
7. методологию анализа и синтеза корреляционно-иммунных и устойчивых булевых функций;
8. методологию анализа и синтеза алгебраически иммунных булевых функций.

**Уметь:**

1. применять на практике алгебраические, комбинаторные, вероятностные и спектральные методы анализа криптографических булевых функций;
2. формулировать простейшие алгебраические, комбинаторные, теоретико-кодовые задачи, решение которых необходимо для вычисления, сравнения или оценки криптографических параметров булевых функций;
3. применять метод быстрого преобразования Адамара (Фурье) для анализа криптографических свойств булевых функций;
4. применять методы декодирования кодов Рида-Маллера для анализа криптографических свойств булевых функций.

**Владеть:**

1. навыками использования в практических целях теоретических результатов;
2. навыками применения теорем, описывающих основные криптографические классы булевых функций;
3. навыками использования современных математических методов анализа и синтеза криптографических булевых функций;

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 3 з.е., в том числе 72 академических часов, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

**6.** Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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)**  **Виды контактной работы, часы** | | | **Самостоятельная работа обучающегося,**  **часы** |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |
| 1. Основные способы представления булевых функций и соотношения, связывающие их основные параметры. | **6** | 2 | 2 | 4 | **2** |
| 1. Преобразование Уолша-Адамара (Фурье) булевой функции. Основные свойства спектрального представления булевой функции. | **6** | 2 | 2 | 4 | **2** |
| 1. Основные свойства функций автокорреляции и взаимной корреляции. | **6** | 2 | 2 | 4 | **2** |
| 1. Алгебраические и комбинаторные параметры, характеризующие групповую эквивалентность булевых функций. | **6** | 2 | 2 | 4 | **2** |
| 1. Нелинейность булевых функций. Алгебраические, комбинаторные, спектральные свойства максимально-нелинейных и платовидных функций. | **8** | 3 | 3 | 6 | **2** |
| 1. Линейные коды, исправляющие ошибки. Коды Рида-Маллера и их свойства. | **12** | 5 | 5 | 10 | **2** |
| 1. Корреляционная иммунность и устойчивость булевых функций. | **14** | 6 | 6 | 12 | **2** |
| 1. Алгебраическая иммунность булевых функций. | **10** | 4 | 4 | 8 | **2** |
| 1. Совершенно уравновешенные булевы функции. | **10** | 4 | 4 | 8 | **2** |
| 1. Математические методы анализа криптографических булевых функций | **14** | 6 | 6 | 12 | **2** |
| Промежуточная аттестация: зачет | **16** | - | - | - | **16** |
| **Итого** | **108** | **36** | **36** | **72** | **36** |

**7. Фонд оценочных средств (ФОС)для оценивания результатов обучения по дисциплине (модулю)**

7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Задания для текущего контроля успеваемости не предусмотрены.

7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

**Вопросы к экзамену**.

1. Булевы функции и способы их представлений (таблица, ДНФ, КНФ, АНФ). Существенные и несущественные переменные. Основные параметры булевых функций. Понятие производной булевой функции. Теорема об алгебраической степени производной. Понятие сужения булевой функции и понятие подфункции.
2. Алгебраическая нормальная форма (АНФ) булевой функции и ее параметры. Соответствие Мебиуса. Теорема о вычислении коэффициентов АНФ. Классы линейных, аффинных, симметричных и монотонных функций.
3. Понятие функциональной разделимости. Теорема К.Шеннона о числе функционально разделимых функций.
4. Теорема МакЭлиса о делимостивеса булевой функции на степень 2.
5. Теорема о связи веса булевой функции и ее алгебраической степени.
6. Теорема о границе веса для почти всех булевых функций.
7. Преобразование Фурье и преобразование Уолша булевой функции. Формулы обращения. Связь спектров Фурье и Уолша. Спектры Уолша аффинных и симметричных функций. Булевы функции с непересекающимися спектрами.
8. Теорема Титсуорта-критерий спектра Уолша (Фурье) булевой функции.
9. Теорема о суммировании спектральных коэффициентов Уолша и экспонент булевых функций по смежным классам линейных подпространств (по плоскостям).
10. Матрицы Адамара и матрицы Адамара-Сильвестра. Теорема о быстром преобразовании Адамара (Фурье).
11. Функции взаимной корреляции и автокорреляции булевых функций. Их основные свойства. Совершенно некоррелированные булевы функции. Теорема о связи совершенной некоррелируемости и свойства непересекаемости спектров булевых функций.
12. Теорема о взаимной корреляции и ее следствия.
13. Теорема о спектре Уоша (Фурье) суммы булевых функций.
14. Групповая эквивалентность булевых функций. Понятие группы инерции булевой функции. Лемма Бернсайда. Групповые инварианты. Построение классификаций булевых функций. Теорема Диксона.
15. Теорема о тривиальности группы инерции относительно полной аффинной группы для почти всех булевых функций.
16. Линейные трансляторы булевых функций. Пространство линейных трансляторов. Теорема о вырождении булевой функции с нетривиальным пространством линейных трансляторов. Алгебраически вырожденные булевы функции и их свойства.
17. Нелинейность булевых функций. Понятие максимально-нелинейной булевой функции (четное и нечетное число переменных). Основные свойства максимально нелинейных функций. Теорема о вычислении нелинейности булевой функции.
18. Понятие бент-функции. Примеры бент-функций. Теорема о дуальной бент-функции.
19. Первый матричный критерий для бент-функций.
20. Второй матричный критерий для бент-функций.
21. Теорема о верхней границе алгебраической степени бент-функции.
22. Бент-функции на основе конструкции Майорана-Макфарланда.
23. Линейные коды, исправляющие ошибки, и их основные параметры. Порождающая и проверочная матрицы линейного кода. Код Хэмминга и его декодирование. Понятие дуального кода и его параметры. Примеры дуальных кодов. Циклические коды. Порождающий и проверочный полиномы циклического кода.
24. Стандартное расположение линейного кода. Алгоритм декодирования, использующий стандартное расположение, и его параметры.
25. Основные неравенства, связывающие параметры линейных кодов (Хэмминга, Синглтона,Плоткина, Варшамова-Гилберта).
26. Весовая функция линейного кода. Теорема МакВильямс о весовой функции дуального кода.
27. Бент-коды и ихсвойства.
28. Коды Рида-Маллера, их основные параметры и свойства.
29. Алгоритм Рида декодирования кодов Рида-Маллера.
30. Алгоритм декодирования кода Рида-Маллера первого порядка, использующий быстрое преобразование Адамара.
31. Понятие корреляционной иммунности (устойчивости) порядка m булевой функции от n переменных. Весовой критерий корреляционной иммунности.
32. Понятие корреляционной иммунности (устойчивости) порядка m булевой функции от n переменных. Спектральный критерий корреляционной иммунности.
33. Теорема о делимости спектральных коэффициентов Уолша корреляционно-иммунной (устойчивой) булевой функции на степень 2. Верхняя граница для нелинейности корреляционно-иммунных и устойчивых булевых функций.
34. Теорема Зигенталера о верхней границе алгебраических степеней корреляционно-иммунных и устойчивых булевых функций.
35. Понятие ортогональной таблицы и ее простейшие свойства. Теорема о связи корреляционно-иммунных (устойчивых) булевых функций и ортогональных таблиц.
36. Аннигиляторы булевых функций и аннуляторы булевых функций. Теорема об алгебраическом строении аннулятора булевой функции. Порядок алгебраической иммунности булевой функции.
37. Теорема о верхней границе для порядка алгебраической иммунности булевой функции.
38. Понятие совершенно уравновешенной булевой функции и понятие булевой функции дефекта нуль. Примеры. Критерий совершенной уравновешенности булевой функции.
39. Теорема о необходимых и достаточных условиях совершенной уравновешенности сдвиг-композиции пары булевых функций.
40. Корреляционный метод криптоанализа. Примеры.

**Экзаменационный билет** состоит из двух вопросов и задачи, например

1. Доказать теорему о вычислении коэффициентов булевой функции (теорема о преобразовании Мебиуса).
2. Доказать теорему Зигенталера о верхней границе алгебраической степени корреляционно-иммунной (устойчивой) функции.
3. Доказать, что невырожденная квадратичная булева функция является бент-функцией.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)** | | | | |
| Оценка  РО и соответствующие виды оценочных средств | 2 | 3 | 4 | 5 |
| **Знания**  *Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения**  *Экзамен* | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки  (владения, опыт деятельности)**  *Экзамен* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки (владения), применяемые при решении задач |

|  |  |
| --- | --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** | |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**   1. теоретические основы спектрального метода анализа(Фурье) криптографических булевых функций; 2. теоретические основы алгебраических методов анализа криптографических булевых функций; 3. теоретические основы комбинаторных методов анализа криптографических булевых функций 4. теоретические основы групповой эквивалентности булевых функций; 5. основы алгебраической и метрической теории полиномиальных кодов Рида-Маллера.   **Уметь:**   1. применять на практике алгебраические, комбинаторные, вероятностные и спектральные методы анализа криптографических булевых функций; 2. формулировать простейшие алгебраические, комбинаторные, спектральные, теоретико-кодовые задачи, решение которых необходимо для вычисления, сравнения или оценки криптографических параметров булевых функций.   **Владеть:**   1. навыками использования в практических целях теоретических результатов, описывающих взаимные связи алгебраических, комбинаторных и криптографических параметров булевых функций. | ОПК-1.Б |
| **Знать:**   1. методологию анализа и синтеза максимально-нелинейных булевых функций; 2. методологию анализа и синтеза корреляционно-иммунных и устойчивых булевых функций; 3. методологию анализа и синтеза алгебраически иммунных функций;   **Уметь:**   1. применять метод быстрого преобразования Адамара (Фурье) для анализа криптографических свойств булевых функций; 2. применять методы декодирования кодов Рида–Маллера для анализа криптографических свойств булевых функций.   **Владеть:**   1. навыками применения теорем, описывающих основные криптографические классы булевых функций; | ОПК-2.Б |
| **Владеть:**   1. навыками использования современных математических методов анализа и синтеза криптографических булевых функций(систем булевых функций); | ПК-2.Б |

8. Ресурсное обеспечение:

Основная литература:

1. Логачев О.А. Криптографические свойства булевых функций. М.: Макс-ПРЕСС, 2007.
2. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии. М: ЛЕНАНД, 2015.

Дополнительная литература:

1. Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях. Математические вопросы кибернетики. Выпуск 11, М: ФИЗМАТЛИТ, 2002, с. 91-148.
2. Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. М: МЦНМО, 2011.
3. Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М: КУРС, 2017.

Информационные справочные системы: https://cryptography.ru/

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания - русский.

10. Преподаватель: Доцент кафедры Информационной безопасности факультета ВМК МГУ О.А.Логачев.

11. Автор программы: доцент кафедры Информационной безопасности факультета ВМК МГУ О.А.Логачев.