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 /
«__» _____2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Алгебраические коды

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

01.04.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Перспективные методы искусственного интеллекта
в сетях передачи и обработки данных

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №7, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.
Дисциплина входит в магистерскую образовательную программу «Перспективные методы искусственного интеллекта в сетях передачи и обработки данных» как дисциплина по выбору, изучается в 1-м семестре.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть):
Изучение дисциплины базируется на освоении знаний по дискретной математике, компьютерным сетям, системам программирования в объеме, соответствующем основным образовательным программам бакалавриата по укрупненной группе направлений и специальностей 02.00.00 «Компьютерные и информационные науки» и другим направлениям подготовки бакалавриата.

3. Результаты обучения по дисциплине (модулю):

Планируемые результаты обучения по дисциплине (модулю)		
Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***
ОПК-1. Способен решать актуальные задачи фундаментальной и прикладной математики	ОПК-1.1. Приобретает и адаптирует математические, естественнонаучные, социально-экономические, общеинженерные знания и знания в области когнитивных наук для решения основных, нестандартных задач создания и применения искусственного интеллекта ОПК-1.2. Решает основные, нестандартные задачи создания и применения искусственного интеллекта, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением	ОПК-1.1. З-1. Знает инструментальные среды, программно-технические платформы для решения профессиональных задач ОПК-1.1. У-1. Умеет применять инструментальные среды, программно-технические платформы для решения профессиональных задач ОПК-1.2. З-1. Знает принципы разработки оригинальных программных средств для решения профессиональных задач ОПК-1.2. У-1. Умеет разрабатывать оригинальные программные средства для решения задач в области создания и применения искусственного интеллекта

	математических, естественно-научных, социально□экономических, общеинженерных знаний и знаний в области когнитивных наук	
ОПК-2. Способен совершенствовать и реализовывать новые математические методы решения прикладных задач	ОПК-2.1. Использует основные инструменты прикладной статистики для решения задач профессиональной деятельности ОПК-2.2. Выбирает оптимальные инструменты статистического анализа данных для решения прикладных задач интеллектуального анализа данных	ОПК-2.1. З-1. Знает фундаментальные научные принципы и методы исследований ОПК-2.1. У-1. Умеет адаптировать с целью практического применения фундаментальные и новые научные принципы и методы исследований ОПК-2.2. З-1. Знает особенности решения профессиональные задачи на основе применения новых научных принципов и методов исследования ОПК-2.2. У-1. Умеет разрабатывать, контролировать, оценивать и исследовать компоненты профессиональной деятельности; планировать самостоятельную деятельность в решении профессиональных задач

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 72 академических часа на контактную работу обучающихся с преподавателем – 36 академических часов занятий лекционного типа, 36 академических часов занятий практического типа. 36 академических часов на самостоятельную работу обучающихся.

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

5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды

учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Номинальные трудозатраты обучающегося**		**Всего академических часов**	**Форма текущего контроля успеваемости***
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы	**Самостоятельная работа обучающегося, академические часы**		

	Занятия лекционного типа	Занятия семинарского типа			**(наименование)**
Тема 1. Теория сравнений	1	1	1	3	опрос
Тема 2. Функция Эйлера	1	1	1	3	опрос
Тема 3. Первообразные корни и индексы	2	2	2	6	опрос
Тема 4. Группа	2	2	2	6	опрос
Тема 5. Подгруппа	2	2	2	6	опрос
Тема 6. Кольца поля	2	2	2	6	опрос
Тема 7. Поля Галуа	2	2	2	6	опрос
Тема 8. Теоремы о полях Галуа	2	2	2	6	опрос
Тема 9. Введение в теорию кодирования	2	2	2	6	опрос
Тема 10. Линейные коды	2	2	2	6	опрос
Тема 11. Кодирование и декодирование линейного кода	2	2	2	6	опрос
Тема 12. Операции над кодами	2	2	2	6	опрос
Тема 13. Границы параметров кодов	2	2	2	6	опрос
Тема 14. Коды, построенные на основе матриц Адамара	2	2	2	6	опрос
Тема 15. Мажоритарное декодирование	2	2	2	6	опрос
Тема 16. Коды, двойственные кодам Хэмминга.	2	2	2	6	опрос
Тема 17. Коды Рида-Маллера	2	2	2	6	опрос
Тема 18. Циклические коды	1	1	1	3	опрос
Тема 19. Коды Боуза-Чоудхури-Хоквингема (коды БЧХ)	1	1	1	3	опрос
Тема 20. Коды с максимально достижимым кодовым расстоянием (МДР-коды)	1	1	1	3	опрос
Тема 21. Линейные переключательные схемы	1	1	1	3	опрос
Другие виды самостоятельной работы (отсутствуют)	—	—			—

Промежуточная аттестация (экзамен)					
Итого	*36*		*36*	108	—

5.2. Содержание разделов (тем) дисциплины

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1.Теория сравнений	Теория сравнений. Определение. Свойства сравнений, полная и приведенная системы вычетов. Теоремы о свойствах систем вычетов.
2.	Тема 2.Функция Эйлера	Функция Эйлера . Определение. Мультипликативность и вычисление функции Эйлера. Теоремы Эйлера и Ферма. Пример применения в криптосистемах с открытым ключом.
3.	Тема 3.Первообразные корни и индексы	Первообразные корни и индексы. Показатель, которому принадлежит число по некоторому модулю. Связь сравнимости чисел со сравнимостью их показателей. Показатели чисел по модулю m, как делители функции Эйлера. Первообразные корни. Модули, по которым существуют первообразные корни.Число первообразных корней.Индексы. Аналогия между индексами и логарифмами. Основные теоремы об индексах.
4.	Тема 4.Группа	Группа. Определение группы. Единичный и обратный элементы. Порядок группы, порядок элемента группы. Показатель группы. Циклическая группа и порядки ее элементов. Примеры групп. Когда приведенная система вычетов является циклической группой?
5.	Тема 5 Подгруппа	Подгруппа. Примеры подгрупп. Смежные классы. Разложение группы по подгруппе.Фактор-группа.Теорема Лагранжа.Нормальные делители. Изоморфизм и гомоморфизм групп.
6.	Тема 6.Кольца и поля	Кольца и поля. Определение кольца. Делители нуля. Область целостности. Определение поля, характеристика поля.Подполе.Примеры колец и полей.Идеал. Примеры идеалов. Идеалы поля.
7.	Тема 7.Поля Галуа	Поля Галуа. Определение поля и построение поля по модулю неприводимого многочлена.Расширение поля, степень расширения.Мультипликативная группа поля.Элементы поля, как корни многочлена $X^{q^m} - X$. Теоремы

		Эйлера и Ферма. Теорема Вильсона. Цикличность мультипликативной группы поля.Аддитивная группа поля.Поле как векторное пространство. Базис поля.
8.	Тема 8. Теоремы о полях Галуа	Теоремы о полях Галуа. Минимальный многочлен; неприводимость, делимость на минимальный многочлен. Существование минимального многочлена для пр извольног элемента поля $GF(q)$. Делимость многочлена $X^{q^m} - X$ на неприводимый многочлен над $GF(q)$. Делимость многочлена $X^{q^m} - X$ на многочлен $X^{q^n} - X$. Элементы β и β^q как корни одного и того же многочлена. Сопряженные элементы поля Галуа. Циклотомические классы. Подполе поля $GF(q^m)$. Степени неприводимых делителей многочлена $X^{q^m} - X$. Порядок корней неприводимого многочлена и порядок неприводимого многочлена. Примитивный многочлен. Изоморфизм полей. Автоморфизмы поля Галуа. Группа автоморфизмов (группа Галуа) поля Галуа. Порядок группы Галуа. Связь между подгруппами группы автоморфизмов с подполями поля Галуа.
9.	Тема 9.Введение в теорию кодирования	Локальная защита:механизмы разграничения уровней доступа, аутентификация и авторизация пользователей, управление доступом к ресурсам. Сетевая защита: файерволлы и фильтры, управление активностью сетевых служб. Криптография и цифровая подпись. PAM. Режим суперпользователя.
10.	Тема 10.Линейные коды	Линейные коды. Определение линейного кода как подпространства. Ортогональные подпространства. Минимальное расстояние и минимальный вес кода. Порождающая и проверочная матрицы кода, их приведённо-ступенчатые формы и связь между ними. Информационные и проверочные символы кода. Связь проверочной матрицы линейного кода с минимальным расстоянием d.
11.	Тема 11.Кодирование и декодирование линейного кода	Кодирование и декодирование линейного кода. Информационный вектор и его умножение на порождающую матрицу. Синдром. Синдромы и смежные классы в разложении пространства по кодовому подпространству. Стандартное расположение, лидеры смежных классов. Совершенные коды.
12.	Тема 12.Операции над кодами	Операции над кодами. Удлинение, укорочение линейного кода. Выкалывание. Расширение линейного кода. Пополнение и выбрасывание.

12.	Тема 13.Границы параметров кодов	Границы параметров кодов. Граница Варшамова-Гилберта (вывод для линейных кодов). Границы Синглтона, Хэмминга, Плоткина и Элайса. Другие границы. Оценка сумм биномиальных коэффициентов, асимптотическая форма границ.
14.	Тема 14.Коды, построенные на основе матриц Адамара	Коды, построенные на основе матриц Адамара. Мощность и корректирующая способность.Построение матриц Адамара. Матрицы Адамара и граница Плоткина.
15.	Тема 15.Мажоритарное декодирование	Мажоритарное декодирование. Разделенные проверки. Реализация кодового расстояния.
16.	Тема 16.Коды, двойственные кодам Хэмминга	Коды, двойственные кодам Хэмминга. Кодовое расстояние и мажоритарное декодирование.
17.	Тема 17.Коды Рида-Маллера	Коды Рида-Маллера Порождающая матрица. Порядок кода Рида-Маллера. Кодовое расстояние. Кодирование и декодирование.
18.	Тема 18.Циклические коды	Циклические коды. Кольцо $F[x]/(x^n-1)$ многочленов по модулю многочлена x^n-1. Циклическое подпространство, циклический код, как идеал. Порождающий многочлен. Проверочный многочлен.Порождающая и проверочная матрицы циклического кода, их приведённо-ступенчатые формы и связь между ними. Кодирование циклического кода. Задание циклического кода корнями его порождающего многочлена. Длина и число проверочных символов циклического кода.
19.	Тема 19.Коды Боуза-Чоудхури-Хоквингема (коды БЧХ)	Коды Боуза-Чоудхури-Хоквингема (коды БЧХ). Определение кода БЧХ. Длина кода. Гарантированное и истинное кодовое расстояние кода БЧХ. Число информационных символов кода БЧХ. Двоичные коды БЧХ. Декодирование двоичного кода БЧХ, исправляющего две ошибки. Общий случай декодирования двоичного кода.Многочлен локаторов ошибок.Алгоритм декодирования Питерсона-Цирлера.Тождества Ньютона. Основная теорема декодирования. Сложность декодирования. Декодирование недвоичных кодов БЧХ.
20.	Тема 20.Коды с максимально достижимым кодовым расстоянием (МДР-коды)	Коды с максимально достижимым кодовым расстоянием (МДР-коды.Информационные совокупности кода. Связь между информационными совокупностями кода и кодовым расстоянием МДР-кода. Дуальный код МДР-кода.Укорочение и выкалывание МДР-кода.Миноры порождающей матрицы. Коды Рида-Соломона. Удлинение кодов Рида-Соломона. Проверочные матрицы удлиненных кодов. Информационный многочлен и

		компоненты кодового вектора. Декодирование кодов Рида-Соломона. Исправление пачек ошибок. Каскадные коды.
21.	Тема 21.Линейные переключательные схемы	Линейные переключательные схемы. Умножение и деление многочленов посредством регистров сдвига с линейными обратными связями.Применение для кодирования и декодирования. Схемы умножения на константу поля Галуа и сопровождающая матрица. Мажоритарное декодирование посредством регистра сдвига с линейными обратными связями. Основные сведения о методах диагностики посредством переключательных схем.

6. Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости, критерии и шкалы оценивания (в отсутствие утвержденных соответствующих локальных нормативных актов на факультете)

Вопросы к опросу
1.Теория сравнений
2. Функция Эйлера
3. Первообразные корни и индексы
4. Группа
5. Подгруппа
6. Кольца и поля
7. Поля Галуа
8. Теоремы о полях Галуа
9. Двоичный симметричный и стирающий каналы
10. Кодовое расстояние
11. Исправление и обнаружение ошибок
12. Исправление стираний
13. Метод исчерпания
14. Код Хэмминга
15. Линейные коды
16. Кодирование и декодирование линейного кода
17. Операции над кодами

18. Границы параметров кодов
19. Коды, построенные на основе матриц Адамара
20. Мажоритарное декодирование
21. Коды, двойственные кодам Хэмминга
22. Коды Рида-Маллера
23. Циклические коды
24. Коды БЧХ
25. МДР-коды
26. Линейные переключательные схемы

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

Вопросы к экзамену
1.Теория сравнений
2. Функция Эйлера
3. Первообразные корни и индексы
4. Группа
5. Подгруппа
6. Кольца и поля
7. Поля Галуа
8. Теоремы о полях Галуа
9. Введение в теорию кодирования. Двоичный симметричный и стирающий каналы. Кодовое расстояние. Исправление и обнаружение ошибок. Исправление стираний. Метод исчерпания. Код Хэмминга
10. Линейные коды
11. Кодирование и декодирование линейного кода
12. Операции над кодами
13. Границы параметров кодов
14. Коды, построенные на основе матриц Адамара
15. Мажоритарное декодирование
16. Коды, двойственные кодам Хэмминга
17. Коды Рида-Маллера
18. Циклические коды
19. Коды Боуза-Чоудхури-Хоквингема (коды БЧХ)

20. Коды с максимально достижимым кодовым расстоянием (МДР-коды)
21. Линейные переключательные схемы

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания *(виды оценочных средств: опрос, тесты)*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *(виды оценочных средств: практические задания)*	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) *(виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)*	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

7. Ресурсное обеспечение:

7.1. Перечень основной и дополнительной литературы

Основная литература

1. Сагалович Ю.Л. Введение в алгебраические коды. М.: ИППИ РАН, 2010. – 302 с.

Дополнительная литература

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986. – 576 с.
3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М.: Связь. 1979. – 744 с.
4. Ван дер Варден Б.Л. Алгебра. М.: Наука. 1976. – 648 с.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир. 1976. – 593 с.
6. Виноградов И.М. Основы теории чисел. М.: Наука, 1972. – 408 с.
7. Бухштаб А.А. Теория чисел. М.: Просвещение, 1966. – 385 с.

7.2.Перечень лицензионного программного обеспечения, в том числе отечественного производстваПри реализации дисциплины может быть использовано следующее программное обеспечение:

1. Операционная система ALT Linux MATE Starterkit 9 лицензияGPL
2. Операционная система Microsoft Windows 10 Education академическая лицензия

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
2. http://www.openet.ru - Российский портал открытого образования

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://asvk.cs.msu.ru

7.5. Описание материально-технического обеспечения.

Образовательная организация, ответственная за реализацию данной Программы, располагает соответствующей материально -технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

доцент, к.ф.-м.н. Гуров С.И.