АННОТАЦИЯ ДИСЦИПЛИНЫ

АЛГЕБРАИЧЕСКИЕ КОДЫ И КРИПТОСИСТЕМЫ

44.03.05 «Педагогическое образование» профили подготовки «Информатика. Математика»

(код направления (специальности) подготовки)

6 семестр

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Освоение студентами основных положений теории алгебраических кодов криптосистем, формирование знаний и навыков в области криптографических методов защиты информации на основе помехоустойчивых кодов, ознакомление студентов с кругом задач классической и современной алгебры и теории чисел; прояснить роль алгебраических понятий во взаимосвязи с другими математическими дисциплинами; сформировать у студентов элементы математической культуры, которые смогут обеспечить ясное понимание смысла и значения разделов математики, изучаемых в школе;
- Подготовка педагогов, обладающих высокой алгебраической культурой, готовых и умеющих применять полученные знания в обучении, в научных исследованиях и при решении прикладных задач, активно участвующих в процессе образования и науки

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Учебная дисциплина «Алгебраические коды и криптосистемы» относится к разделу «Дисциплины по выбору» учебного плана.

Для изучения и освоения дисциплины нужны знания из курсов алгебры, теории чисел, теории вероятностей. Этот курс является естественным продолжением курсов алгебры и теории чисел. Курс показывает как основные положения алгебры и теории чисел прилагаются в теории кодирования и криптосистемах.

Изучение курса позволит студентам получить представление о конструкциях шифров и систем защиты, основанных на применении теории помехоустойчивых кодов, методов их построения, способов анализа стойкости к различного вида математическим атакам, способах организации защищенных систем передачи данных с помощью криптографических протоколов, базирующихся на кодовых шифрах

Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при дипломных работ, связанных с математическим моделированием в области защиты информации.

В части курса, посвященной теории кодирования, студенты знакомятсяс базовыми понятиями теории линейных кодов (основные понятия, кодирование и декодирование линейных кодов, границы объемов кодов, методы построения кодов), а также теории циклических кодов (кольцо многочленов над полем Галуа, определение циклического кода, необходимое и достаточное условие существования циклического кода с порождающим

многочленом g(x), кодирование и декодирование циклических кодов, коды Хэмминга, коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды Рида-Соломона). Эти классы кодов наиболее часто применяются на практике. Теория кодирования самым тесным образом связана с дискретным анализом, теорией групп, теорией Галуа, конечными геометриями, теорией графов, теорией блок-схем, криптографией.

Вторая часть курса посвящена введению в криптологию, теорема Шеннона о существовании совершенно секретных шифров, а также основные криптосистемы с открытыми ключами: криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма, криптосистема Шамира, криптосистема, основанная на эллиптических кривых, цифровые подписи, базирующиеся на основных криптосистемах. Здесь же рассматриваются вопросы применения теории кодирования в криптографии (кодовые асимметричные криптосистемы, проблемы аутентификации, блоковые шифры, проблемы распределения секретов).

В третьей части курса, посвященной сжатию данных излагаются основные методы сжатия данных – методы побуквенного кодирования (коды Фано, Хаффмена, Шеннона), критерий однозначности кодирования, теорема Шеннона; основные методы адаптивного кодирования (методы Лемпела-Зива, код “стопка книг”, арифметический код).

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования: ПК-11

- готовность использовать систематизированные теоретические и практические знания для определения и решения исследовательских задач в области образования

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Кодирование: основные понятия и идеи эффективного помехоустойчивого кодирования. Экономный код Фано - Шеннона.

Префиксные коды. Свойства префикса и однозначное декодирование.

Оптимальный код. Код Хаффмена. Понятие энтропии информации.

Линейные коды. Помехоустойчивое кодирование. Код с общей проверкой на четность. Код с повторением.

Код Хэмминга (n,k), исправляющий одну ошибку.

Кодовое расстояние. Геометрическая интерпритация кодов. Исправление и обнаружение ошибок.

Групповые коды. Порождающая и проверочная матрицы кода.

Декодирование по синдрому. Коды, исправляющие несимметрические ошибки.

Циклические коды. Порождающий многочлен.

Коды Боуза - Чоудхури - Хоквингема (БЧХ).

Алгебраические криптосистемы. Основы теории чисел в криптографии. Сравнения первой степени. Теорема Эйлера - Ферма.

Простые числа. Разложимость целых чисел на множители. Проблема больших простых чисел и их значение в криптосистемах.

Поточные криптосистемы.

Криптосистема с открытым ключом.

Криптосистема с закрытым ключом. Криптосистема без передачи ключа.

Идентификация и аутентификация. Электронная подпись. Управление ключами.

Элементы шифрования и криптоанализа. Модели систем шифрования. Простейшие шифры.

Алгебраическое шифрование. Стандарты DES, AES.

Практическое использование криптографии.

5. **ВИД АТТЕСТАЦИИ** – зачет

6. **КОЛИЧЕСТВО ЗАЧЕТНЫХ ЕДИНИЦ - 3**

Составитель: доцент кафедры МА Куранова Н.Ю.
должность, ФИО, подпись

Заведующий кафедрой математического анализа В.В. Жиков
название кафедры ФИО, подпись

Председатель
учебно-методической комиссии направления М.В.Артамонова

Директор института М.В. Артамонова Дата: 17.03.2016

Печать института