Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«_28_» ___08___ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«АЛГЕБРАИЧЕСКИЕ КОДЫ И КРИПТОСИСТЕМЫ»

Направление подготовки «44.03.05 Педагогическое образование»

Профиль/программа подготовки «Математика. Информатика»

Уровень высшего образования БАКАЛАВРИАТ

Форма обучения ОЧНАЯ

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
6	5/180		54		81	экзамен -45 ч.
Итого	5/180		54		81	45

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины (модуля) является:

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.

Задачи освоения дисциплины:

создать представление о круге задач, решаемых с помощью кодовых криптосистем и соответствующих криптографических протоколов;

рассмотреть основные способы построения кодовых криптосистем; рассмотреть основные методы математических атак на шифры и криптографические протоколы, построенные на базе помехоустойчивых кодов;

овладеть теоретико- информационными, алгебраическими и комбинаторными методами анализа стойкости кодовых шифров и соответствующих криптографических протоколов к математическим атакам

сформировать знания, умения и навыки кодирования различных видов информации;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина (модуль) «Алгебраические коды и криптосистемы» относится к блоку "Дисциплины по выбору".

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 (МОДУЛЯ)

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

Выпускник должен обладать следующими профессиональными компетенциями (ПК):

- Готовность использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования (ПК-11).

"В соответствии с профессиональным стандартом педагога (приказ Министерства труда и социальной защиты населения РФ № 544н от 18.10.2013г.) преподаватели в средней школе при разработке и реализации программ учебных дисциплин в рамках основной общеобразовательной программы, а также при планировании и проведении учебных занятий должны владеть общепользовательскими и общепедагогическими ИКТ-компетентностями (ИКТ - информационно-коммуникационные технологии). "

В результате освоения дисциплины обучающийся должен:

Знать:

конструкции кодов и кодовых криптосистем;

основные теоретико- информационные и алгебраические методы анализа стойкости кодовых криптосистем;

основные задачи, решаемые с использованием кодовых криптосистем, методы теории кодирования для решения задач передачи информации по каналам связи с шумами;

методы теории информации для решения задач передачи информации по каналам связи без шума.

Уметь:

осуществлять процедуру шифрования и расшифрования с использованием кодовых криптосистем; определять тип стойкости кодового шифра (теоретическая или вычислительная);

конструировать теоретически и вычислительно стойкие кодовые криптосистемы; конструировать защищенную систему передачи данных с использованием кодовых шифров и соответствующих криптографических протоколов,

оценивать возможности применения и применять методы передачи, хранения и защиты информации для решения конкретных прикладных задач (в частности создания цифровых подписей, защиты паролей).

Владеть:

основными методами теории помехоустойчивого кодирования для передачи информации по каналам связи с помехами такими как методы кодирования и декодирования линейных кодов, методы кодирования и декодирования циклических кодов (кодов БЧХ, Рида-Соломона);

навыками построения кодов и криптосистем для конкретных помехоустойчивых кодов; методами анализа стойкости кодовых криптосистем;

основными методами теории сжатия данных – методы кодирования для стационарных источников, адаптивные методы кодирования, универсальные методы.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Кодирование: основные понятия и идеи эффективного помехоустойчивого кодирования. Экономный код Фано - Шеннона.	6	1		2			6		0.5/25	
2.	Префиксные коды. Свойства префикса и однозначное декодирование.	6	2		4			4		1/25	Рейтинг–контроль №1
3.	Оптимальный код. Код Хаффмена. Понятие энтропии информации.	6	3		2			4		0.5/25	
4.	Линейные коды. Помехоустойчивое кодирование. Код с общей проверкой на четность. Код с повторением.	6	4		4			4		1/25	
5.	Код Хэмминга (n,k), исправляю-	6	5		2			6		0.5/25	

	щий одну ошибку.										
6.	Кодовое расстояние. Геометрическая интерпритация кодов. Исправление и обнаружение ошибок.	6	6		4			4		1/25	Рейтинг-контроль №2
7.	Групповые коды. Порождающая и проверочная матрицы кода.	6	7		2			4		0.5/25	
8.	Декодирование по синдрому. Коды. исправляющие несимметрические ошибки.	6	8		4			4		1/25	
9.	Циклические коды. Порождающий многочлен. Коды Боуза - Чоудхури - Хоквингема (БЧХ).	6	9		2			6		0.5/25	
10.	Алгебраические криптосистемы. Основы теории чисел в криптографии. Сравнения первой степени. Теорема Эйлера - Ферма.	6	10		4			4		1/25	
11.	Простые числа. Разложимость целых чисел на множители. Проблема больших	6	11		2			4		0.5/25	

	простых чисел и их значение в криптосистемах.										
12.	Поточные криптосистемы.	6	12		4			4		1/25	
13.	Криптосистема с открытым ключом.	6	13		2			4		0.5/25	Рейтинг-контроль №3
14.	Криптосистема с закрытым ключом. Криптосистема без передачи ключа.	6	14		4			4		1/25	
15.	Идентификация и аутентификация. Электронная подпись. Управление ключами.	6	15		2			4		0.5/25	
16.	Элементы шифрования и криптоанализа. Модели систем шифрования. Простейшие шифры.	6	16		4			4		1/25	
17.	Алгебраическое шифрование. Стандарты DES, AES.	6	17		2			4		0.5/25	
18.	Практическое использование криптографии.	6	18		4			7		1/25	
Всего					54			81		13/25	экзамен

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации программы дисциплины «Алгебраические коды и криптосистемы» используются различные методы изложения лекционного материала в зависимости от конкретной темы – вводная, установочная, подготовительная лекции, лекции с применением техники обратной связи, лекция-беседа. С целью проверки усвоения студентами необходимого теоретического минимума, проводятся экспресс - тесты по лекционному материалу в письменной форме. Практические занятия предназначены для освоения и закрепления теоретического материала, изложенного на лекциях. Практические занятия направлены на приобретение навыка решения конкретных задач, расчетов на основе имеющихся теоретических и фактических знаний. На коллоквиумах обсуждаются теоретические вопросы изучаемого курса. Консультации представляют собой своеобразную форму проведения лекционных занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. Самостоятельная работа студентов направлена на закрепление полученных навыков и на приобретение новых теоретических и фактических знаний, выполняется в читальном зале библиотеки и в домашних условиях, подкрепляется учебно- методическим и информационным обеспечением (учебники, учебно-методические пособия, конспекты лекций). Практикуется самостоятельная работа по постановке и решению индивидуальных оригинальных прикладных задач. Студенты готовятся к участию в ежегодной студенческой олимпиаде по математике. Для активизации образовательной деятельности с целью формирования и развития профессиональных навыков обучающихся, используются формы проблемного, контекстного, индивидуального и междисциплинарного обучении.

.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Текущий контроль - рейтинг-контроль №1,2,3
Промежуточная аттестация - экзамен (6 сем)

Задания к рейтинг-контролю

Рейтинг-контроль № 1.
ТЕМА: Однозначное кодирование. Оптимальный код
Постановка задачи:. Экономный код Фано - Шеннона. Префиксные коды. Свойства префикса и однозначное декодирование. Оптимальный код. Код Хаффмена. Понятие энтропии информации

Ход работы:

1. Закодируйте сообщения с заданными вероятностями троичным кодом Фано и кодом Хаффмена по основанию 4. Построить дерево, оценить погрешности относительно равномерного кода.
   0,21; 0,2; 0,17; 0,16; 0,12; 0,08; 0,04; 0,02.
2. Закодировать по коду Шеннона сообщения с длинами слов
   L(2, 2, 2, 4, 4, 4)
   для r=2 и r=3
3. Выбрать максимальное по числу элементов подмножество B множества A с условием, что двоичные разложения наименьшей длины чисел из B представляют собой: а) префиксный код; б) однозначно декодируемый код:

A={ 5,7,9,10,12,14,17,23,24}

4. Будет ли код однозначно декодируемым?

{1112, 10201121, 20, 01202, 22, 2012010, 2001}

5. Закодировать сообщение А, декодировать сообщение В по Хэммингу. В каждом случае выписать порождающую и проверочную матрицы

A=10110110001

B=10111101110001

Рейтинг-контроль № 2.

ТЕМА:. Линейные коды. Помехоустойчивое кодирование.

Постановка задачи: Код с общей проверкой на четность. Код с повторением. Код Хэмминга (n,k), исправляющий одну ошибку

Ход работы:

1. Закодируйте сообщения с заданными вероятностями троичным кодом Фано и кодом Хаффмена по основанию 4. Построить дерево, оценить погрешности относительно равномерного кода.
   0,21; 0,2; 0,17; 0,16; 0,12; 0,08; 0,04; 0,02.
2. Закодировать по коду Шеннона сообщения с длинами слов
   l,(2, 2, 2, 4, 4, 4)
3. Выбрать максимальное по числу элементов подмножество В множества А с условием, что двоичные разложения наименьшей длины чисел из В представляют собой: а) префиксный код; б) однозначно декодируемый код:

A={ 5,7,9,10,12,14,17,23,24}

4. Построить по методу Хэмминга кодовое слово для сообщения

a=100010011

5. Восстановить по методу Хэмминга сообщение
   b=11011100110

Рейтинг-контроль 3

ТЕМА:. Порождающие и проверочные матрицы линейных кодов.

Постановка задачи. Матричное кодирование. Асимметричные коды

Ход работы.

1. Закодировать сообщение А, декодировать сообщение В. В каждом случае выписать порождающую и проверочную матрицы

A=10110110001

B=10111101110001

2. В сообщении было замещение 0 на 1, восстановить его (n=6, l=7):

101100

110101

111110

3. В сообщении было выпадение 1-го символа, восстановить его (n=6, l=7)

01101

10100

11111

4. В сообщении была вставка 1-го символа, восстановить его (n=6, l=7)

1001101

1110100

1111110

Тест 1

1. Какое количество информации по Хартли может содержать система, информационная емкость которой определяется десятичным числом 1250.
2. Найти среднее количество информации по Шеннону в системе со следующим вероятностным распределением $\vec{p}\,(1/2;1/4;1/4)$.
3. Какое максимальное количество информации по Шеннону содержит система со следующим вероятностным распределением $\vec{p}\,(0{,}2;0{,}8)$.
4. Сравните условную и безусловную энтропии системы.

   Варианты ответов:

   a) $H_Y(X) \geq H(X)$;

   b) $H_Y(X) \leq H(X)$.
5. Определить дифференциальную энтропию системы с заданной плотностью распределения вероятностей: $f(x) = \begin{cases} x,\ x \in (0;1) \\ 0,\ x \notin (0;1) \end{cases}$.

Тест 2

1. Выберите наиболее реальную модель сигнала.

   Варианты ответов:

   a) случайный процесс;
   b) детерминированный сигнал;
   c) случайный сигнал.
2. Сколько видов модуляции гармонического сигнала существует?

   Варианты ответов:

   a) два;
   b) бесконечно много;
   c) три.
3. Какой спектр имеет периодический сигнал?

   Варианты ответов:

   a) сплошной;
   b) линейчатый.
4. Определить шаг равномерной дискретизации для сигнала с ограниченным спектром

   $f_{\max} = 50 гц$.

Тест 3

1. Что происходит с длиной сообщения при эффективном кодировании?

   Варианты ответов:

   a) увеличивается;
   b) остается прежней;
   c) уменьшается.
2. Как изменяется эффективность кода при увеличении длины блока при блоковом кодировании?

   Варианты ответов:

   a) не убывает;
   b) не изменяется;
   c) не возрастает.
3. Закодировать сообщение 100110 кодом с проверкой четности.

   Варианты ответов:

   a) 1001100;
   b) 10011011;
   c) 1001101.
4. Закодировать число 13 кодом Хэмминга (4,7).

   Варианты ответов:

a) 1010101;
b) 1110101;
c) 1011101.

5. Исправить ошибку в кодовом слове 1010111 (код Хэмминга (4,7)) и найти передаваемое десятичное число.

Варианты ответов:

a) 15;
b) 13;
c) 9.

Тест 4

1. Какое устройство системы передачи информации обеспечивает эффективность ее передачи?

Варианты ответов:

a) модулятор;
b) кодер источника;
c) кодер канала.

2. Какое устройство системы передачи информации обеспечивает достоверность ее передачи?

Варианты ответов:

a) кодер канала;
b) кодер источника;
c) модулятор.

3. Что является информационной характеристикой только канала связи?

a) скорость передачи информации;
b) пропускная способность.

4. Определить пропускную способность дискретного канала связи без шума, по которому передается 10 сигн./сек. Алфавит сообщений источника состоит из 16 букв

тест 5

Задача №1.

Составить структурную схему кодера для циклического кода заданного производящим полиномом $p(x)=x^4+x^3+x+1$. Найти комбинацию проверочного кода для информационной последовательности 10011 математическим способом и путем «прогона» через кодер. Пояснить процесс кодирования.

Задача №2.

Составить структурную схему декодера с обнаружением ошибки для циклического кода заданного производящим полиномом $p(x)=x^4+x^3+x+1$. Пришедшая информационная последовательность имеет ошибку в 4 разряде. Показать наличие ошибки в кодовой комбинации математическим способом и путем «прогона» через декодер. Пояснить процесс декодирования и обнаружения.

Задача №3.

Составить структурную схему декодера с исправлением ошибки для циклического кода заданного производящим полиномом $p(x)=x^4+x^3+x+1$. Поступившая информационная последовательность имеет ошибку в 5 разряде. Показать наличие ошибки в кодовой комбинации математическим способом и путем «прогона» через декодер. Пояснить процесс исправления ошибки

тест 6

Для зашифрования текста использовался вращающийся диск, центр которого находится на оси, закрепленной на неподвижном основании. Диск разделен на 32 равных сектора, в

которые в неизвестном порядке вписаны все буквы русского алфавита (по одной в каждый сектор: буквы Е и Ё не различаются). На основании, по одной напротив каждого сектора, выписаны буквы в алфавитном порядке по часовой стрелке. Каждое положение диска, получающееся из исходного поворотом на угол, кратный величине сектора, задает соответствие между буквами на основании и на диске. При зашифровании очередной буквы текста ее заменяли соответствующей ей буквой при текущем положении диска, после чего диск поворачивался на один сектор по часовой стрелке. Укажите, какой из фрагментов полученного шифртекста

У Ш Ц Ш М Ь Г Р У Н В И О Ь Х Ь З Ж И Х С Ж Ы Р О Р Л Й Я О Ш К Ь Э З Д О Е

может соответствовать слову **ШИФРАТОР** в исходном тексте:

В И О Ь Х Ь З Ж

У Ш Ц Ш М Ь Г Р

О Ш К Ь Э З Д О

Ж Ы Р О Р Л Й Я

О Р Л Й Я О Ш К

тест 7

Исходное цифровое сообщение коммерсант шифрует и передает. Для этого он делит последовательность цифр исходного сообщения на группы по пять цифр в каждой и после двух последовательных групп приписывает еще две последние цифры суммы чисел, изображенных этими двумя группами. Затем к каждой цифре полученной последовательности он прибавляет соответствующий по номеру член некоторой целочисленной арифметической прогрессии, заменяя результат сложения остатком от деления его на 10.
Найдите исходное цифровое сообщение по шифрованному сообщению:

4 2 3 4 6 1 4 0 5 3 1 3

тест 8

Задача №1.
Постороить криптосистему с открытым ключом
Задача №2.
Постороить криптосистему с закрытым ключом
Задача №3.
Постороить криптосистему без передачи ключа
Задача №4.
Постороить криптосистему -электронная подпись

.

Тестовый рейтинг-контроль

1 – 10. Определить количество информации (по Хартли), содержащееся в системе, информационная емкость которой характеризуется десятичным числом *Q*. Закодировать это число по двоичной системе счисления.

№	1	2	3	4	5	6	7	8	9	10
Q	500	1000	750	1250	250	1500	650	900	1100	1600

11 – 20. Определить среднее количество информации, содержащееся в сообщении, используемом три независимых символа S_1, S_2, S_3. Известны вероятности появления символов $p(S_1)=p_1$, $p(S_2)=p_2$, $p(S_3)=p_3$. Оценить избыточность сообщения.

№	11	12	13	14	15	16	17	18	19	20
p_1	0,1	0,2	0,3	0,1	0,15	0,1	0,2	0,2	0,05	0,15
p_2	0,15	0,1	0,15	0,3	0,2	0,4	0,25	0,3	0,15	0,25
p_3	0,75	0,7	0,55	0,6	0,65	0,5	0,55	0,5	0,8	0,6

21 – 30. В условии предыдущей задачи учесть зависимость между символами, которая задана матрицей условных вероятностей $P(S_j / S_i)$.

21. $\begin{pmatrix} 0,8 & 0 & 0,2 \\ 0 & 0,5 & 0,5 \\ 0,1 & 0,5 & 0,4 \end{pmatrix}$ **22.** $\begin{pmatrix} 0 & 0,4 & 0,6 \\ 0,7 & 0,1 & 0,2 \\ 0,5 & 0 & 0,5 \end{pmatrix}$ **23.** $\begin{pmatrix} 0,6 & 0,2 & 0,2 \\ 0,3 & 0 & 0,7 \\ 0 & 0,4 & 0,6 \end{pmatrix}$

24. $\begin{pmatrix} 0,2 & 0 & 0,8 \\ 0,5 & 0,1 & 0,4 \\ 0 & 0,3 & 0,7 \end{pmatrix}$ **25.** $\begin{pmatrix} 0,1 & 0,8 & 0,1 \\ 0 & 0,3 & 0,7 \\ 0,4 & 0 & 0,6 \end{pmatrix}$ **26.** $\begin{pmatrix} 0 & 0,2 & 0,8 \\ 0,5 & 0 & 0,5 \\ 0,4 & 0,3 & 0,3 \end{pmatrix}$

27. $\begin{pmatrix} 0,4 & 0 & 0,6 \\ 0,8 & 0,1 & 0,1 \\ 0 & 0,3 & 0,7 \end{pmatrix}$ **28.** $\begin{pmatrix} 0,3 & 0,2 & 0,5 \\ 0 & 0,1 & 0,9 \\ 0,2 & 0 & 0,8 \end{pmatrix}$ **29.** $\begin{pmatrix} 0 & 0,3 & 0,7 \\ 0,1 & 0,3 & 0,6 \\ 0,6 & 0 & 0,4 \end{pmatrix}$

30. $\begin{pmatrix} 0,5 & 0,5 & 0 \\ 0,3 & 0,3 & 0,4 \\ 0 & 0,7 & 0,3 \end{pmatrix}$

31 – 40. Провести кодирование по одной и блоками по две буквы, используя метод Шеннона–Фано. Сравнить эффективности кодов. Данные взять из задач №11 –20.

41 – 50. Алфавит передаваемых сообщений состоит из независимых букв S_i. Вероятности появления каждой буквы в сообщении заданы. Определить и сравнить эффективность кодирования сообщений методом Хаффмана при побуквенном кодировании и при кодировании блоками по две буквы.

№	$P(S_i)$	№	$P(S_i)$
41	(0,6;0,2;0,08;0,12)	46	(0,7;0,2;0,06;0,04)
42	(0,7;0,1;0,07;0,13)	47	(0,6;0,3;0,08;0,02)

43	(0,8;0,1;0,07;0,03)	48	(0,5;0,2;0,11;0,19)
44	(0,5;0,3;0,04;0,16)	49	(0,5;0,4;0,08;0,02)
45	(0,6;0,2;0,05;0,15)	50	(0,7;0,2;0,06;0,04)

51 – 60. Декодировать полученное сообщение c, если известно, что использовался (7, 4) – код Хэмминга. Провести кодирование кодом с проверкой четности.

№	c	№	c
51	1100011	56	1011011
52	1010011	57	1010101
53	1101101	58	0110111
54	1101001	59	1110101
55	1100111	60	1000101

61 – 70. Определить пропускную способность канала связи, по которому передаются сигналы S_j. Помехи в канале определяются матрицей условных вероятностей $P(S_j / S_i)$. За секунду может быть передано $N = 10$ сигналов.

61. $\begin{pmatrix} 0,2 & 0,8 & 0 \\ 0 & 0,2 & 0,8 \\ 0,8 & 0 & 0,2 \end{pmatrix}$ **62.** $\begin{pmatrix} 0,4 & 0,3 & 0,3 \\ 0,3 & 0,4 & 0,3 \\ 0,3 & 0,3 & 0,4 \end{pmatrix}$ **63.** $\begin{pmatrix} 0,7 & 0,3 & 0 \\ 0 & 0,7 & 0,3 \\ 0,3 & 0 & 0,7 \end{pmatrix}$

64. $\begin{pmatrix} 0,2 & 0,4 & 0,4 \\ 0,4 & 0,2 & 0,4 \\ 0,4 & 0,4 & 0,2 \end{pmatrix}$ **65.** $\begin{pmatrix} 0,4 & 0,6 & 0 \\ 0 & 0,4 & 0,6 \\ 0,6 & 0 & 0,4 \end{pmatrix}$ **66.** $\begin{pmatrix} 0,6 & 0,2 & 0,2 \\ 0,2 & 0,6 & 0,2 \\ 0,2 & 0,2 & 0,6 \end{pmatrix}$

67. $\begin{pmatrix} 1/3 & 1/3 & 1/6 & 1/6 \\ 1/6 & 1/6 & 1/3 & 1/3 \end{pmatrix}$ **68.** $\begin{pmatrix} 0,8 & 0,1 & 0,1 \\ 0,1 & 0,8 & 0,1 \\ 0,1 & 0,1 & 0,8 \end{pmatrix}$ **69.** $\begin{pmatrix} 0,4 & 0,4 & 0,1 & 0,1 \\ 0,1 & 0,1 & 0,4 & 0,4 \end{pmatrix}$

70. $\begin{pmatrix} 0,3 & 0,35 & 0,35 \\ 0,35 & 0,3 & 0,35 \\ 0,35 & 0,35 & 0,3 \end{pmatrix}$

Вопросы к экзамену

1. Кодирование: основные понятия и идеи эффективного помехоустойчивого кодирования. Экономный код Фано - Шеннона.
2. Префиксные коды. Свойства префикса и однозначное декодирование.
3. Оптимальный код. Код Хаффмена. Понятие энтропии информации.
4. Линейные коды. Помехоустойчивое кодирование. Код с общей проверкой на четность. Код с повторением.
5. Код Хэмминга (n,k), исправляющий одну ошибку.
6. Кодовое расстояние. Геометрическая интерпритация кодов. Исправление и обнаружение ошибок.
7. Групповые коды. Порождающая и проверочная матрицы кода.
8. Декодирование по синдрому. Коды, исправляющие несимметрические ошибки.
9. Циклические коды. Порождающий многочлен.
10. Коды Боуза - Чоудхури - Хоквингема (БЧХ).
11. Алгебраические криптосистемы. Основы теории чисел в криптографии. Сравнения первой степени. Теорема Эйлера - Ферма.
12. Простые числа. Разложимость целых чисел на множители. Проблема больших простых чисел и их значение в криптосистемах.
13. Поточные криптосистемы.
14. Криптосистема с открытым ключом.
15. Криптосистема с закрытым ключом. Криптосистема без передачи ключа.
16. Идентификация и аутентификация. Электронная подпись. Управление ключами.
17. Элементы шифрования и криптоанализа. Модели систем шифрования. Простейшие шифры.
18. Алгебраическое шифрование. Стандарты DES, AES.
19. Практическое использование криптографии.

Учебно-методическое обеспечение самостоятельной работы студентов

Особое место в овладении данным курсом отводится самостоятельной работе, которая заключается в следующем: –самостоятельное изучение части теоретического материала, теоретическая подготовка к практическим занятиям, систематическое выполнение домашних заданий, выполнение индивидуальных заданий.
В качестве самостоятельной работы по дисциплине «Алгебраические коды и криптосистемы » студенты готовят рефераты по передаче, хранению и кодированию информации по следующим темам:

1. Статистический анализ каналов связи.
2. Критерий Манна - Уитни. Критерий Уилкоксона.
3. Критерий знаков для анализа парных повторных наблюдений.
4. Анализ повторных парных наблюдений с помощью знаковых рангов.

5. Арифметическое кодирование.
6. Арифметический вес. Арифметическое расстояние.
7. Условие обнаружения ошибок. Условие исправления ошибок.
8. Коды с обнаружением ошибок.
9. Коды с исправлением одиночных ошибок.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Название и выходные данные (автор, вид издания, издательство, издания, количество страниц)	Год издания	Количество экземпляров в библиотеке университета	Наличие в электрон-ной библиотеке ВлГУ	Количество студентов, использующих указанную литературу	Обеспеченность студентов литерату-рой, %
1	2	3	4	5	6	7
Основная литература						
1	А.В. Бабаш. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие . 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.	2014		ЭБС «znanium» http://znanium.com/ ISBN 978-5-9963-1139-2	20	100%
2	В.М. Белов, С.Н. Новиков, О.И. Солонская.Теория информации. Курс лекций: Учебное пособие для вузов - М.: Гор. линия-Телеком, 2012. - 143 с	2012		ЭБС «znanium» http://znanium.com/ ISBN 978-5-9912-0237-4	20	100%
3	Рябко Б.Я., Фионов А.Н.. Криптографические методы защиты информации: Учебное пособие для вузов / - 2-е изд., стереотип. - М.: Гор. линия-Телеком, 2012. - 229 с.	2012		ЭБС «znanium» http://znanium.com ISBN 978-5-9912-0286-2.	20	100%
Дополнительная литература						
1	Панин, В. В. Основы теории информации [Электронный ресурс] : учебное пособие для вузов / В. В. Панин. - 4-е изд. (эл.). - М. : БИНОМ. Лаборатория знаний, 2012. - 438 с.	2012		ЭБС «znanium» http://znanium.com/ ISBN 978-5-9963-0759-3.	20	100%
2	Березкин Е.Ф. Основы теории информации и кодирования. Лабораторный практикум: Учебно-методическое пособие - М.:НИЯУ "МИФИ", 2009. - 84 с	2009		ЭБС «znanium» http://znanium.com/ ISBN:978-5-7262-1120-6	20	100%
3	Чечёта С.И. Введение в дискретную теорию информации и кодирования: учебное издание. - М.: МЦНМО, 2011. - 224 с.	2011		ЭБС «Консультант студента» http://www.studentlibrary.ru/book/ ISBN 978-5-94057-701-0.	20	100%
4	Березкин Е.Ф. .Основы теории информации и кодирования: Учебное пособие / - М.:НИЯУ "МИФИ", 2010. - 312 с	2010		ЭБС «znanium» http://znanium.com/ ISBN 978-5-7262-1294-4	20	100%
5	Душин В. К. Теоретические основы информационных процессов и систем: Учебник / - 5-е	2014		ЭБС «Консультант студента» http://www.studentl	20	100%

	изд. - М.: Издательско-торговая корпорация "Дашков и К°", 2014. - 348 с			ibrary.ru/book/ ISBN 978-5-394-01748-3.		

Интернет-ресурсы:

Сайт "Теория кодирования в Новосибирском государственном университете" по адресу http://www.codingtheory.gorodok.net.

Сайт "Math Tree" : каталог математических интернет ресурсов (раздел "Теория кодирования") по адресу http://www.mathtree.ru.

http://math.ru/lib/bmkvant/30

Периодические издания

1. Журнал "Алгебраические коды" http:// http://arxiv.org/
2. журнал "Проблемы передачи информации http://www.mathnet.ru/php/journal.phtml?jrnid=ppi&option_lang=rus"
3. Научно-популярный физико-математический журнал "Квант" http://kvant.mccme.ru/key.htm
4. Журнал "Известия Российской академии наук. Серия математическая"
5. http://www.mathnet.ru/php/journal.phtml?jrnid=im&option_lang=rus
6. Сибирский математический журнал http://www.emis.de/journals/SMZ/attention.htm
7. Журнал «Математические заметки» http://www.ams.org/mathscinet/search/journaldoc.html?jc=MATZA1

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории для проведения лекционных и семинарских занятий, средства мультимедиа

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 44.03.05 «ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ» ПРОФИЛЬ « МАТЕМАТИКА. ИНФОРМАТИКА »

Рабочую программу составил Куранова Наталья Юрьевна

Рецензент
(представитель работодателя) МАОУ Гимназия №3 , Мартьянова Г.И
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры _____
Протокол № 9 от 15.05.2016 года
Заведующий кафедрой Жиков В.В.
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 44.03.05 «ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ» ПРОФИЛЬ « МАТЕМАТИКА. ИНФОРМАТИКА »
Протокол № 5 от 29.08.16 года
Председатель комиссии директор ПИ Артамонова М. В.
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____