Министерство науки и высшего образования 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
«_12_» _08_____ 2018г.

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 промежуточной аттестации (экзамен/зачет/зачет с оценкой)
6	4/144		54		45	Экзамен 45
Итого	4/144		54		45	Экзамен 45

Владимир 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины 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

Дисциплина «Алгебраические коды и криптосистемы» относится к вариативной части учебного плана.

Пререквизиты дисциплины. Дисциплина опирается на знания предметов основной образовательной программы среднего (полного) общего образования: «Алгебра», «Алгебра и начала анализа» Базируется на знаниях, полученных в рамках школьного курса математики и ранее изученных дисциплин среднего профессионального образования.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП

Код формируемых компетенций	Уровень освоения компетенции	Планируемые результаты обучения по дисциплине характеризующие этапы формирования компетенций (показатели освоения компетенции)
1	*2*	*3*
ПК -11	Частичный	ЗНАТЬ • об актуальных проблемах развития образования и педагогических наук; знает назначение и особенности использования основных методик психолого-педагогического и методического исследования • функциями и содержанием научно-методической работы педагога, учителя математики и физики, с организацией научно-методической работы в организации общего образования, понимает роль методического объединения. УМЕТЬ • пользоваться базовыми исследовательскими процедурами психологии, педагогики, частных методик, выполняет учебно-исследовательские задачи, осознавая возможности и границы применения исследовательских методов. • анализировать образовательный процесс, собственную деятельность, выявляя проблемы, которые могут быть решены в рамках проектно-исследовательской деятельности; способен на основе выявленной проблемы сформулировать исследовательскую задачу ВЛАДЕТЬ • опытом научно-методической работы во взаимодействии с методическим объединением учителей математики и информатики; • опытом выступления перед учителями или однокурсниками с сообщением по проблеме исследования. • навыком сбора, изучения, критического анализа, обобщения и систематизации информации по теме учебно-исследовательской работы; способен грамотно описать результаты исследования в жанре курсовой работы и представить работу на публичной защите.

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часов.

№ п/п	Наименование тем и/или разделов/тем 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, форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	СРС		
1.	Кодирование: основные понятия и идеи эффективного помехоустойчивого кодирования. Экономный код Фано - Шеннона.	6	1		2		2	1/50%	
2.	Префиксные коды. Свойства префикса и однозначное декодирование.	6	2		4		3	1/25%	
3.	Оптимальный код. Код Хаффмена. Понятие энтропии информации.	6	3		2		2	1/50%	
4.	Линейные коды. Помехоустойчивое кодирование. Код с общей проверкой на четность. Код с повторением.	6	4		4		3	1/25%	
5.	Код Хэмминга (n,k), исправляющий одну ошибку.	6	5		2		2	1/50%	Рейтинг-контроль 1
6.	Кодовое расстояние. Геометрическая интерпритация кодов. Исправление и обнаружение ошибок.	6	6		4		3	1/25%	
7.	Групповые коды. Порождающая и проверочная матрицы кода.	6	7		2		2	1/50%	
8.	Декодирование по синдрому. Коды, исправляющие несимметрические ошибки.	6	8		4		3	1/25%	
9.	Циклические коды. Порождающий многочлен. Коды Боуза - Чоудхури - Хоквингема (БЧХ).	6	9		2		2	1/50%	
10.	Алгебраические криптосистемы. Основы теории чисел в криптографии. Сравнения первой степени. Теорема Эйлера - Ферма.	6	10		4		3	1/25%	Рейтинг-контроль 2
11.	Простые числа. Разложимость целых чисел на множители. Проблема больших простых чисел и их значение в криптосистемах.	6	11		2		2	1/50%	
12.	Поточные криптосистемы.	6	12		4		3	1/25%	

13.	Криптосистема с открытым ключом.	6	13		2		2	1/50%	
14.	Криптосистема с закрытым ключом. Криптосистема без передачи ключа.	6	14		4		3	1/25%	
15.	Идентификация и аутентификация. Электронная подпись. Управление ключами.	6	15		2		2	1/50%	
16.	Элементы шифрования и криптоанализа. Модели систем шифрования. Простейшие шифры.	6	16		4		3	1/25%	
17.	Алгебраическое шифрование. Стандарты DES,. AES.	6	17		2		2	1/50%	Рейтинг-контроль 3
18.	Практическое использование криптографии.	6	18		4		3	1/25%	
Всего за 6 семестр		6			54		45	18/33%	Экзамен
Наличие в дисциплине КП/КР					-				
Итого по дисциплине					54		45	18/33%	45

Содержание практических занятий по дисциплине

Раздел 1. Кодирование: основные понятия и идеи эффективного помехоустойчивого кодирования. Экономный код Фано - Шеннона

Тема 1. Помехоустойчивость кода

Тема 2. Двоичные и троичные коды Шеннона. Дерево кода

Раздел 2. Префиксные коды. Свойства префикса и однозначное декодирование

Тема 1. Понятие префикса. Коды без запятой Понятие постфикса

Тема 2. Однозначнодекодируемые коды. Дерево однозначнодекодируемых кодов

Раздел 3. Оптимальный код. Код Хаффмена. Понятие энтропии информации

Тема 1. Понятие полноты кода. Оптимальное кодирование. Оптимальный код Хаффмена

Тема 2. Понятие энтропии в кодировании

Раздел 4. Линейные коды. Помехоустойчивое кодирование. Код с общей проверкой на четность. Код с повторением

Тема 1. Линейное пространство кодов. Помехи и кодирование. Базовые коды

Тема 2. Код с проверкой на четность и код с повторением

Раздел 5. Код Хэмминга (n,k), исправляющий одну ошибку

Тема 1. Линейный код Хэмминга (7,4)

Тема 2. Линейный код (8,4)

Тема 3. Кодирование и декодирование по Хэммингу

Раздел 6. Кодовое расстояние. Геометрическая интерпретация кодов. Исправление и обнаружение ошибок

Тема 1. Связь кодового расстояния с помехоустойчивостью кода.

Тема 2. Аппарат исправления и обнаружения ошибок в линейных кодах

Раздел 7 Групповые коды. Порождающая и проверочная матрицы кода

Тема 1. Понятие порождающей матрицы и ее свойства

Тема 2. Понятие проверочной матрицы и ее свойства

Раздел 8. Декодирование по синдрому. Коды, исправляющие несимметрические ошибки.

Тема 1. Синдром и вектор ошибки в помехоустойчивом кодировании

Тема 2. Код с выпадающим символом, код со вставкой символа

Раздел 9. Циклические коды. Порождающий многочлен. Коды Боуза - Чоудхури - Хоквингема (БЧХ).

Тема 1. Построение циклических кодов.

Тема 2. БЧХ код, код Рида-Маллера

Раздел 10. Алгебраические криптосистемы.

Тема 1. Основы теории чисел в криптографии. Сравнения первой степени. Теорема Эйлера - Ферма.

Тема 2. Простые числа. Разложимость целых чисел на множители. Проблема больших простых чисел и их значение в криптосистемах

Тема 3. Поточные криптосистемы

Тема 4. Криптосистема с открытым ключом

Тема 5. Криптосистема с закрытым ключом. Криптосистема без передачи ключа.

Тема 6. Идентификация и аутентификация. Электронная подпись. Управление ключами.

Раздел16. Элементы шифрования и криптоанализа. Модели систем шифрования. Простейшие шифры.

Тема 1. Криптоустойчивость системы.

Тема 2. Защита информации. Шифр Хилла

Раздел 17. Алгебраическое шифрование. Стандарты DES, AES.

Тема 1. Понятие алгебраического шифрования. Алгебраические структуры

Тема 2. Современные стандарты шифрования

Раздел 18. Практическое использование криптографии.

Тема 1. Прикладные задачи криптографии

Тема 2. Передача и защита информации

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Алгебраические коды и криптосистемы*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

- *Интерактивная лекция (тема №1,5,7);*
- *Групповая дискуссия (тема №1,2,6,11);*

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. 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 успеваемости

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 A, декодировать сообщение B 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 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. 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

Контрольная работа

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_i. 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.

Темы (рекомендуемая литература, формы контроля)

1. Статистический анализ каналов связи. [1,2,3]

2. Критерий Манна - Уитни. Критерий Уилкоксона. [1,2,3]
3. Критерий знаков для анализа парных повторных наблюдений. [1,2,3]
4. Анализ повторных парных наблюдений с помощью знаковых рангов. [1,2,3]
5. Арифметическое кодирование. [1,2,3]
6. Арифметический вес. Арифметическое расстояние. [1,2,3]
7. Условие обнаружения ошибок. Условие исправления ошибок. [1,2,3]
8. Коды с обнаружением ошибок. [1,2,3]
9. Коды с исправлением одиночных ошибок. [1,2,3]

Контрольные вопросы для самостоятельной оценки качества освоения дисциплины

1. Определение кода и способа помехоустойчивого кодирования (СПхК). Отличие кодов от шифров. Простейший СПхК.
2. Параметры помехоустойчивых кодов (ПхК) и их сущность. Критерии, используемые для оценки эффективности ПхК и СПхК.
3. Классификация ПхК.
4. Классификация и краткая характеристика способов (принципов) построения (задания) и алгоритмов декодирования ПхК.
5. Первичные коды: определение, способы построения, основные параметры и классификация кодов.
6. Эффективные коды: определение, способы построения, основные параметры, достоинства, недостатки и области применения.
7. Префиксные коды: определение, способы построения, классификация кодов, основные свойства, достоинства, недостатки и область применения.
8. Линейные блоковые коды (ЛБК): определение, основные свойства, способы задания (построения), достоинства, недостатки.
9. Циклические коды (ЦК): определение, основные свойства и способы построения.
10. Порождающие и проверочные матрицы ЦК: назначение, способы построения и характеристики (параметры) матриц. Взаимосвязь матриц.
11. Порождающие и проверочные полиномы ЦК: требования, предъявляемые к данным полиномам, назначение и основные параметры полиномов.
12. Сущность алгоритма мажоритарного декодирования ЦК при формировании системы раздельных проверок (СРП). Достоинства и недостатки данного алгоритма декодирования.
13. сущность алгоритма мажоритарного декодирования ЦК при формировании системы связанных проверок (ССвП). Достоинства и недостатки данного алгоритма.
14. Сущность алгоритма декодирования ЦК с использованием весовой оценки остатка от деления $R(x) = \frac{F'(x)}{P(x)}$. Достоинства и недостатки данного алгоритма декодирования.
15. Циклические коды Файра: назначение, способ построения и алгоритмы декодирования. Способ построения укороченных ЦК Файра, основные свойства данных кодов, их достоинства и недостатки.
16. БЧХ-коды: способ построения, алгоритмы декодирования, достоинства и недостатки.
17. Циклические коды Рида-Соломона: определение, назначение, способ построения, алгоритмы декодирования, достоинства и недостатки.
18. Многомерные коды: определение, классификация и области применения.

19. Матричные коды: определение, способы построения, параметры, достоинства и недостатки.
20. Итеративные коды: определение, принцип построения и параметры двумерного итеративного кода. Достоинства и недостатки итеративных кодов.
21. Каскадные коды: определение, способы (варианты) построения двухкаскадного кода, параметры, достоинства и недостатки данных кодов.
22. Перемежители – деперемежители кодовых символов: назначение, классификация, основные параметры, достоинства и недостатки.
23. Сущность способов помехоустойчивого кодирования при «жестком» и «мягком» принятии решения на выходе Д.К.С.
24. Сверточные коды (СК): определение, основные параметры и способы их задания.
25. Классификация СК. Достоинства и недостатки СК с алгоритмом порогового декодирования (ПД).
26. Классификация алгоритмов декодирования СК и их краткая характеристика.
27. Сущность многопорогового (на примере двух порогов) алгоритма декодирования СК. Достоинства и недостатки данного алгоритма декодирования.
28. Классификация и сущность принципов построения формирователей проверочных символов систематических и несистематических СК.
29. Принципы построения анализаторов синдромной последовательности при «жестком» и «мягком» принятии решения на выходе ДКС.
30. назначение, определение и основные свойства разностных Δ-ков совершенных разностных множеств.

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ	
		Количество экземпляров изданий в библиотеке ВлГУ в соответствии с ФГОС ВО	Наличие в электронной библиотеке ВлГУ
1	2	3	4
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
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
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.
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.
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
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.
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

7.2. Периодические издания

1. Научно-популярный физико-математический журнал "Квант"
http://kvant.mccme.ru/key.htm
2. Журнал "Известия Российской академии наук. Серия математическая"
http://www.mathnet.ru/php/journal.phtml?jrnid=im&option_lang=rus
3. Сибирский математический журнал
http://www.emis.de/journals/SMZ/attention.htm
4. Журнал «Математические заметки»
http://www.ams.org/mathscinet/search/journaldoc.html?jc=MATZA1
5. Журнал вычислительной математики и математической физики.
6. Вестник Самарского государственного технического университета. Серия физико-математические науки

7.3. Интернет-ресурсы

1. https://ru.wikipedia.org/wiki
2. http://neerc.ifmo.ru/wiki/index.php?
3. http://www.mccme.ru/free-books/pdf/alfutova.pdf
4. www.intuit.ru/studies/courses/616/472/info
5. http://www.exponenta.ru/educat/class/courses/student/la/examples.asp тесты для самоконтроля - fen.distant.ru/test/math/3/test-3.htm
6. http://wwwcdl.bmstu.ru/fn1/LinAlg.pdf
7. http://www.resolventa.ru/metod/student/linalg.htm
8. Издательство МЦНМО [Электронный ресурс]. – URL: www.mccme.ru/free-books. Свободно распространяемые книги.
9. Математическая библиотека [Электронный ресурс]. – URL: www.math.ru/lib.Большая библиотека, содержащая как книги, так и серии брошюр, сборников. В библиотеке представлены не только книги по математике, но и по физике и истории науки.
10. Образовательный математический сайт [Электронный ресурс]. – URL: http://www.exponenta.ru Содержит материалы по работе с математическими пакетами Mathcad, MATLAB, MathematicalMaple и др., методические разработки, примеры решения задач, выполненные с использованием математических пакетов. Форум и консультации для студентов и школьников.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий *лекционного типа, занятий практического/лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы (указать необходимое)*. Практические работы проводятся в 230, 241, 237

Учебные аудитории для проведения лекционных и семинарских занятий- 230, 129

Рабочую программу составил доц. Куранова Н.Ю. _____

Рецензент
(представитель работодателя) и.о. директора Захарова Е.А.

Программа рассмотрена и одобрена на заседании кафедры МОиИТ
Протокол № 10 от 29.06.18 года
Заведующий кафедрой к. ф.-м. н., доц. Евсеева Ю.Ю. _____

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 44.03.05 «Педагогическое образование»
Протокол № 1 от 28.08.18 года
Председатель комиссии к. филол. н., доц. Артамонова М.В. _____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

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_____