МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа и операторных уравнений

Каменский М.И.
подпись, расшифровка подписи
25.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.10 Методы кодирования и криптологии и разработка программного обеспечения информационно-коммуникационных технологий

1. Код и наименование направления подготовки: 02.04.01 Математика и компьютерные науки

2. Профиль подготовки: Математическое и компьютерное моделирование, Математические методы и компьютерные технологии в естествознании, экономике и управлении

3. Квалификация выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра функционального анализа и операторных уравнений

6. Составители программы: Завгородний Михаил Григорьевич**,** канд. физ-мат. наук, доцент

7. Рекомендована: НМС математического факультета, протокол № 0500–06 от 25.05.2023

8. Учебный год: *2023-2024* **Семестр(ы):** 2

9.Цели и задачи учебной дисциплины:

Целью изучения предмета «Математические методы и модели теории кодирования и криптологии и разработка на их основе программного обеспечения информационно-коммуникационных технологий» является приобретение основных знаний и умений построения помехоустойчивых кодов и использования современных криптографических методов и алгоритмов защиты информации; приобретение навыков составления эффективных алгоритмов и их программирования для решения типовых задач кодирования, обеспечивающих помехоустойчивую запись и передачу по каналам связи данных, для решения типовых задач защиты информации современными методами шифрования с асимметричным ключом.

Основными задачами изучения дисциплины являются:

- изучение методов и алгоритмов построения помехоустойчивых линейных кодов и реализация их в виде программ;
- изучение методов и алгоритмов построения помехоустойчивых линейных циклических кодов и реализация их в виде программ;
- изучение методов и алгоритмов построения помехоустойчивых кодов БЧХ и реализация их в виде программ;
- изучение быстрых алгоритмов, выполняющих арифметические операции над большими (длинными) целыми числами, и реализация их в виде программного модуля;
- изучение эффективных алгоритмов модулярной арифметики и реализация их в виде программного модуля;
- получение представлений об использовании аналогов полученных программных продуктов в современной криптосистеме RSA, а также для проверки чисел на простоту и для факторизации чисел.

10. Место учебной дисциплины в структуре ООП: (*блок Б1, базовая или вариативная часть, к которой относится дисциплина; требования к входным знаниям, умениям и навыкам; дисциплины, для которых данная дисциплина является предшествующей)*

Дисциплина входит в обязательную часть блока 1. «Дисциплины (модули)». Для изучения и освоения дисциплины нужны знания, приобретенные магистрами ранее при обучении в бакалавриате, а именно, знания из курсов алгебры и теории чисел, технологии программирования и работы на ЭВМ, теории вероятностей и других. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться в курсе «Технологии разработки наукоемкого программного обеспечения», в учебной практике по получению первичных навыков научно-исследовательской работы и при выполнении дипломных работ, связанных с математическим моделированием в области защиты информации при ее передаче по каналам связи.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен самостоятельно создавать прикладные программные средства на основе современных информационных технологий и	ОПК-3.1	Обладает фундаментальными знаниями в области прикладного программирования и информационных технологий	Знать: основные методы и алгоритмы построения помехоустойчивых кодов, основные методы и алгоритмы криптографии и компьютерной алгебры, связанные с модулярной арифметикой; Уметь: разрабатывать эффективные и готовые к программной реализации алгоритмы помехоустойчивого кодирования, современного криптографического преобразования данных и

	сетевых ресурсов, в том числе отечественного производства			криптоанализа; Владеть: навыками реализации разработанных алгоритмов в виде программных модулей.
		ОПК-3.2	Умеет использовать прикладные программные средства в профессиональной деятельности	Знать: область применения методов и моделей помехоустойчивого кодирования, современного криптографического преобразования данных и криптоанализа; Уметь: использовать полученные знания для защиты данных при записи, хранении на внешних носителях и при передаче по каналам связи; Владеть: навыками применения программных продуктов кодирования и криптографии в своей профессиональной деятельности для защиты информации.
		ОПК-3.3	Имеет практический опыт применения программных средств, используемых при построении математических моделей в естественных науках	Знать: методы формализации математических моделей в областях помехоустойчивого кодирования, криптографии, компьютерной алгебры и некоторых современных систем шифрования с асимметричным ключом; Уметь: выбрать эффективные программные продукты для решения поставленной практической задачи в областях помехоустойчивого кодирования и современной криптографии, Владеть: навыками практического применения программных продуктов, реализующих математические модели помехоустойчивого кодирования и современной криптографии с асимметричным ключом.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **— 4/144.**

Форма промежуточной аттестации*(зачет/экзамен)* *зачет с оценкой.*

13. Виды учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			2 семестр
Аудиторные занятия		56	56
в том числе:	лекции	28	28
	практические	-	-
	лабораторные	28	28
Самостоятельная работа		88	88
в том числе: курсовая работа (проект)		-	-
Форма промежуточной аттестации *(зачет с оценкой – __час.)*			зачет
Итого:		144	144

13.1. Содержание дисциплины

№	Наименование раздела	Содержание раздела дисциплины

п/п	дисциплины	
1	Предмет и задачи курса. Методы, модели и алгоритмы помехоустойчивых линейных кодов.	Структура курса. Терминология. Методы обнаружения и исправления ошибок при передаче данных по каналам связи. Расстояние Хэмминга. Помехоустойчивые линейные коды, их построение и декодирование. Программная реализация алгоритмов построения и декодирования помехоустойчивых линейных кодов.
2	Методы, модели и алгоритмы помехоустойчивых линейных циклических кодов.	Построение и декодирование помехоустойчивых линейных циклических кодов. Программная реализация алгоритмов построения и декодирования помехоустойчивых линейных циклических кодов.
3	Методы, модели и алгоритмы кодов БЧХ.	Построение и декодирование кодов БЧХ. Программная реализация алгоритмов построения и декодирования кодов БЧХ.
4	Методы, модели и алгоритмы арифметических операций над большими (длинными) целыми числами.	Изучение алгоритмов сложения, вычитания, умножения, деления и возведения в степень больших (длинных) целых чисел. Их программная реализация.
5	Методы, модели и алгоритмы арифметических операций над большими (длинными) целыми числами в кольце вычетов.	Изучение алгоритмов сложения, вычитания, умножения и возведения в степень больших (длинных) целых чисел в кольце вычетов. Изучение одного из алгоритмов шифрования с асимметричным ключом. Их программная реализация.
6	Быстрые алгоритмы умножения и возведения в степень целых чисел в кольце вычетов.	Изучение алгоритмов Монтгомери умножения и возведения в степень в кольце вычетов. Программная реализация алгоритмов Монтгомери и основанного на них алгоритма асимметричного шифрования.
7	Быстрые алгоритмы вычисления НОД и обратных элементов в конечном поле.	Изучение бинарных алгоритмов нахождения НОД. составление программы на его основе. Программная реализация вычисления НОД и обратных элементов в конечном поле.
8	Методы факторизации числа и проверка простоты.	Метод пробных делителей, метод Ферма, метод Лемана.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Предмет и задачи курса. Методы, модели и алгоритмы помехоустойчивых линейных кодов.	6	6	17	29
2	Методы, модели и алгоритмы помехоустойчивых линейных циклических кодов.	4	4	9	17
3	Методы, модели и алгоритмы кодов БЧХ.	4	4	18	26
4	Методы, модели и алгоритмы арифметических операций над большими (длинными) целыми числами.	4	4	17	25
5	Методы, модели и алгоритмы арифметических операций над большими (длинными) целыми	2	2	9	13

	числами в кольце вычетов.				
6	Быстрые алгоритмы умножения и возведения в степень целых чисел в кольце вычетов.	4	4	9	17
7	Быстрые алгоритмы вычисления НОД и обратных элементов в конечном поле.	2	4	9	15
8	Методы факторизации числа и проверка простоты.	2	--	–	2
	Итого	28	28	88	144

14. Методические указания для обучающихся по освоению дисциплины

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции и лабораторные занятия, которые предполагают самостоятельную работу студентов по данной дисциплине. Обучающимся предлагается ряд индивидуальных заданий, которые необходимо выполнять в течение семестров для закрепления пройденного материала и успешного освоения дисциплины. Предусмотрены домашние задания и оформление отчетов выполнения лабораторных заданий, а также дополнительные задания для сильных студентов.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

№ п/п	Источник
1	*Кудряшов, Борис Давидович. Теория информации : учебное пособие / Б.Д. Кудряшов .— СПб [и др.] : Питер, 2009 .— 314 с. : ил. — (Учебник для вузов).*
2	*Завгородний, Михаил Григорьевич. Программирование. Криптографические алгоритмы : учебное пособие / М.Г. Завгородний, С.П. Майорова .— Воронеж : Издательский дом ВГУ, 2018 .— 96 с.*
3	*Маховенко, Елена Борисовна. Теоретико-числовые методы в криптографии : учебное пособие для студ. вузов, обуч. по специальностям группы "Информ. безопасность" / Е. Б. Маховенко .— М.: Гелиос АРВ, 2006 .— 318 с.*

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
3	*Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2007. – Ч. 2 – 130 с.*
4	*Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2008. – Ч. 3 – 102 с.*
5	*Кнут, Дональд Эрвин. Искусство программирования [Т.2: Получисленные алгоритмы] / Дональд Э. Кнут ; под общ. ред. Ю.В. Козаченко .— М. : Вильямс, 2004. — 3-е изд. — 2004.— 828 с*
6	*Василенко, Олег Николаевич. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко ; Ин-т проблем информационной безопасности МГУ .— М. : МЦНМО, 2003 .— 325 с.*

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

№ п/п	Источник
1	www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .

18. Материально-техническое обеспечение дисциплины:
(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Лекционная аудитория (доска, мел, маркеры), Компьютерный класс (14-15 компьютеров), программное обеспечение (Microsoft Visual Studio; Free Pascal (GNU General Public License (GPL); Python 2/3 (Python Software Foundation License (PSFL)), мультимедийный проектор.

19. Фонд оценочных средств:

Задания открытого типа:

1. Расстояние Хэмминга двух кодовых слов 01011011 и 11101011 равно ____.

Ответ: ***3***.

2. Минимальное расстояние кода, состоящего из четырех кодовых слов: 00000, 10110, 01011, 11101, равно _____.

Ответ: ***3***.

3. Сообщение кодируется следующими четырьмя кодовыми словами: 00000, 10110, 01011, 11101. Указанный код обнаруживает не более ____ ошибок.

Ответ: ***2***.

4. Сообщение кодируется следующими четырьмя кодовыми словами: 00000, 10110, 01011, 11101. Указанный код исправляет не более ____ ошибок.

Ответ: ***1***.

5. Линейный двоичный (15,5)-код имеет ____ информационных разрядов и ____ избыточных разрядов.

Ответ: ***5, 10***.

6. Порождающая матрица двоичного линейного кода (15, 4) имеет размеры ____.

Ответ: ***4*15.***

7. Порождающая матрица систематического двоичного линейного кода (4, 3) имеет вид _____.

Ответ: $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

8. Проверочная матрица двоичного линейного кода (15, 4) имеет размеры ____.

Ответ: ***11*15.***

9. Кодовые слова БЧХ-кода, построенного на конечном поле $GF(2^3)$, порожденным неприводимым многочленом $\varphi(x)=x^3+x+1$, имеют ____.двоичных разрядов, из которых _____ разрядов избыточные.

Ответ: ***17, 3.***

10. БЧХ-код (7,4), гарантированно исправляет _____ ошибок.

Ответ: ***1.***

11. При кодировании использовали БЧХ-код (7,4) и значение синдрома ошибок $E(\alpha)$ равно α^3. Это означает, что ошибка произошла в ____ позиции кодового слова.

Ответ: ***4.***

12. Пробное частное двух целых чисел 49439032 и 6439767 равно _____ .

Ответ: $\left[\frac{49}{6}\right]=8$**.**

13. Целая часть числа $\sqrt{2910}$ равна _____ .

Ответ: 53

Вычисление: $x_1=100;\ x_2=\left[\frac{1}{2}\left(100+\left[\frac{2910}{100}\right]\right)\right]=64;\ x_3=\left[\frac{1}{2}\left(64+\left[\frac{2910}{64}\right]\right)\right]=54;$

$x_4=\left[\frac{1}{2}\left(54+\left[\frac{2910}{54}\right]\right)\right]=53;\ x_5=\left[\frac{1}{2}\left(53+\left[\frac{2910}{53}\right]\right)\right]=\left[\frac{1}{2}(53+54)\right]=53.$

14. Известно, что при некотором заданном модуле $N>1000$ величина $(R^{-1})\bmod N$ равна 14, где R – основание системы счисления. Тогда значение $\varphi(2\cdot 5)$ функции Монтгомери равно $\varphi(x)=\frac{x-N\left((xN^{-1})\bmod R\right)}{R}$ равно ____ .

Ответ: 2*5*14=140**.**

15. Величина $17^{1026}\bmod 19$ равна _____ .

Ответ: $17^{1026}\bmod 19=\left((-2)^4\right)^{256}(-2)^2\bmod 19=\left((-3)^4\right)^{64}4\bmod 19=$

$=\left(5^2\right)^{32}4\bmod 19=\left(6^2\right)^{16}4\bmod 19=\left((-2)^4\right)^4 4\bmod 19=1$**.**

16. Элемент ____ является обратным к элементу 7 в кольце вычетов Z_{480}.

Ответ: ***343.***

Задания закрытого типа:

17. Избыточность помехоустойчивого кода – это

Варианты ответов

- разность между количеством кодовых слов и количеством кодируемых информационных слов;
- наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код;

- характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом; (***Верный ответ***)
- число информационных разрядов в кодовом слове.

18. Расстояние Хэмминга – это

Варианты ответов

- число разрядов двух кодовых слов, в которых они различны; (***Верный ответ***)
- расстояние между символами
- наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код;
- характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом;
- число контрольных разрядов в кодовом слове.

19. Минимальное кодовое расстояние – это

Варианты ответов

- число разрядов двух кодовых слов, в которых они различны;
- наименьшее из всех расстояний Хэмминга для любых пар различных кодовых слов, образующих код; (***Верный ответ***)
- характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом;
- число контрольных разрядов в кодовом слове.

20. Линейным двоичным (n,k)-кодом называется

Варианты ответов

- набор из n кодовых слов, расстояние Хэмминга для которых равно k;
- любое k-мерное подпространство пространства Z_2^n; (***Верный ответ***)
- множество k-мерных двоичных векторов, полученное умножением n-мерных двоичных векторов на порождающую матрицу;
- набор из n кодовых слов, минимальное расстояние кода для которых равно k.

21. Матрица является порождающей матрицей линейного кода, если

Варианты ответов

- любая ее строка ортогональна каждому кодовому слову линейного кода;
- любой ее столбец ортогонален каждому кодовому слову линейного кода;
- ее столбцы образуют базис подпространства кодовых слов линейного кода;
- ее строки образуют базис подпространства кодовых слов линейного кода; (***Верный ответ***)

22. Матрица является проверочной матрицей линейного кода, если

Варианты ответов

- любая ее строка ортогональна каждому кодовому слову линейного кода;
- любой ее столбец ортогонален каждому кодовому слову линейного кода; (***Верный ответ***)
- ее столбцы образуют базис подпространства кодовых слов линейного кода;

- ее строки образуют базис подпространства кодовых слов линейного кода;

23. Линейный (n,k) -код называется циклическим, если

Варианты ответов

- каждое кодовое слово линейного кода при циклическом сдвиге его бит не меняется;
- циклический сдвиг бит любого кодового слова также является кодовым словом; (***Верный ответ***)
- проверочная матрица при циклическом сдвиге ее столбцов не меняется;
- проверочная матрица при циклическом сдвиге ее строк не меняется.

24. Порождающим многочленом циклического кода называют

- приведенный многочлен, соответствующий кодовому слова и имеющий наибольшую степень;
- приведенный многочлен, соответствующий кодовому слова и имеющий наименьшую степень; (***Верный ответ***)
- неприводимый многочлен, соответствующий кодовому слова и имеющий наименьшую степень;
- неприводимый многочлен, соответствующий кодовому слова и имеющий наибольшую степень;

25. Код БЧХ – это

Варианты ответов

- линейный код, с порождающей матрицей, построенной Боузом, Рой-Чоудхури и Хоквингемом;
- блоковый код, с порождающей матрицей, построенной Боузом, Рой-Чоудхури и Хоквингемом;
- линейный код, у которого порождающая и проверочная матрицы совпадают;
- циклический код, порождаемый многочленом, имеющим корнями примитивный элемент α поля Галуа $GF(2^m)$, а также степени α^k, $k=\overline{2,t}$, этого примитивного элемента. (***Верный ответ***)

26. При программировании арифметических операций над большими (длинными) целыми числами возникает следующая основная проблема:

Варианты ответов

- ограниченность памяти компьютера;
- необходимость часто переводить числа из одной системы счисления в другую;
- все данные имеют заранее заданный формат; (***Верный ответ***)
- отсутствие библиотек для работы с большими (длинными) целыми числами.

27. В 1000-ичной системе счисления выбор первой цифры неполного частного в алгоритме деления с остатком двух целых чисел 49439032 и 6439767 осуществляется из

Варианты ответов

- 1000 вариантов;
- трех вариантов;

- не более трех вариантов; (***Верный ответ***)
- более 500 вариантов.

28. В массиве $b[s]$ записано число b в двоичную систему счисления. Что вычисляет следующий алгоритм?
    1. Вводим a Полагаем $z = a$.
    2. Цикл при изменении переменной i от $s-1$ до 0 выполняем:
        2.1 Полагаем $z = z^2$.
        2.2 Если $b[i]=1$, то полагаем $z = z * a$.
    3. Выводим z.

Варианты ответов

- вычисляет величину a^{2s};
- вычисляет величину a^b; (***Верный ответ***)
- выполняет умножение a на b по Монтгомери;
- находит НОД(a,b);
- извлекает квадратный корень из числа a.

29. Что вычисляет следующий алгоритм?
    1. Вводим число n.
    2. Полагаем $x = n$.
    3. Цикл
        3.1 Полагаем $z = x$.
        3.2 Полагаем $x = (x + n/x)/2$.
        Выполнять цикл, пока $x < z$.
    4. Выводим z.

Варианты ответов

- вычисляет величину x^{2s};
- вычисляет величину x^m;
- выполняет умножение по Монтгомери;
- переводит число x в двоичную систему счисления;
- извлекает квадратный корень из числа x. (***Верный ответ***)

30. Что вычисляет следующий алгоритм?
    1. Вводим числа a и b.
    2. Полагаем $g = 1$.
    3. Цикл: пока оба числа a и b четные, выполнять: $a = \frac{a}{2}$, $b = \frac{b}{2}$ и $g = 2 * g$.
    4. Цикл: пока $a \neq 0$, выполнять:
        4.1. Цикл: пока число a четное, выполнять: $a = \frac{a}{2}$.

4.2. Цикл: пока число b четное, выполнять: $b = \frac{b}{2}$.

4.3. При $a \geq b$ полагаем $a = a - b$. Иначе $b = b - a$.

5. Выводим $d = g * b$.

Варианты ответов

- вычисляет величину a^{2s};
- вычисляет величину a^b;
- выполняет умножение a на b по Монтгомери;
- находит НОД(a, b); (***Верный ответ***)
- извлекает квадратный корень из числа a.

31. Что вычисляет следующий алгоритм?

1. Вводим числа a, b, N и R.
2. Положим $x = a * b$ и $N' = \left(-N^{-1}\right) \bmod R$.
3. Положим $U = (x * N') \bmod R$.
4. Положим $z = x + N * U$.
5. Положим $f = z / R$.
6. Если $f \geq N$, то полагаем $f = f - N$.
7. Выводим f.

Варианты ответов

- вычисляет величину a^{2s};
- вычисляет величину a^b;
- выполняет умножение a на b по Монтгомери; (***Верный ответ***)
- находит НОД(a, b);
- извлекает квадратный корень из числа a.

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме лабораторных работ.

Промежуточная аттестация проводится в форме зачета и включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

При сдаче зачета
оценка «отлично» - 5 баллов
оценка «хорошо» - 4 балла
оценка «удовлетворительно» - 3 балла
оценка «неудовлетворительно» - 2 балла.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом, владеет методами построения математических моделей в области помехоустойчивого кодирования и криптографии; способен иллюстрировать ответ примерами, фактами, применять теоретические знания для разработки алгоритмов и их программирования.	*Повышенный уровень*	*Отлично*
У обучающегося сформированы знания, умения и навыки построения математических моделей помехоустойчивого кодирования и криптографии; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.	*Базовый уровень*	*Хорошо*
У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	*Пороговый уровень*	*Удовлетвори-тельно*
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	–	*Неудовлетвори-тельно*

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

__.__.__

Направление подготовки / специальность ___02.04.01 Математика и компьютерные науки

Дисциплина__Б1.О.11 Математические методы и модели теории кодирования и криптологии и разработка на их основе программного обеспечения информационно-коммуникационных технологий

Форма обучения _____очная_____
очное, очно-заочное, заочное
Вид контроля _____зачет_____
экзамен, зачет
Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Помехоустойчивые линейные коды. Порождающая и проверочная матрицы

2. Алгоритм Монтгомери умножения в кольце вычетов. Оценка его сложности.

Преподаватель _____ _____.
подпись расшифровка подписи