09.03.02.01.Б1.В-2021-РП

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: институт информационных технологий, машиностроения и автотранспорта
Должность: директор института
Дата: 16.05.2022 21:54:07

Стенин Дмитрий Владимирович

Рабочая программа дисциплины

Теория информации, данные, знания

Направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) 01 Системная интеграция и автоматизация информационных процессов

Присваиваемая квалификация
"Бакалавр"

Формы обучения
очная

Кемерово 2022 г.

1621832750

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационных и автоматизированных производственных систем
Должность: старший преподаватель
Дата: 12.06.2022 16:28:05

Матисов Александр Вениаминович

Рабочая программа обсуждена на заседании кафедры информационных и автоматизированных производственных систем

Протокол № 3/1 от 14.03.2022

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационных и автоматизированных производственных систем
Должность: заведующий кафедрой (к.н)
Дата: 16.06.2022 09:21:53

Чичерин Иван Владимирович

Согласовано учебно-методической комиссией по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии

Протокол № 4/1 от 04.04.2022

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационных и автоматизированных производственных систем
Должность: заведующий кафедрой (к.н)
Дата: 16.06.2022 09:23:13

Чичерин Иван Владимирович

1621832750

1 Перечень планируемых результатов обучения по дисциплине "Теория информации, данные, знания", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-3 - Оптимизация функционирования прикладного программного обеспечения

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Выполняет построение и декодирование линейных блоковых кодов. Выполняет расчёт информационных характеристик дискретных сообщений и пропускной способности каналов связи. Проводит сжатие данных различными методами. Проводит шифрование сообщений.

Результаты обучения по дисциплине:

Знать основные понятия теории информации; информационные характеристики источников сообщений и каналов связи и способы их оценки; основные методы эффективного (оптимального) кодирования и сжатия информации; основные виды помехоустойчивых кодов, методы их построения и декодирования; основные теоремы теории информации; основные понятия криптографии и методы шифрования информации.

Уметь строить и декодировать линейные блоковые коды для обнаружения и исправления ошибок в сообщениях; определять количество информации в дискретных сообщениях; рассчитывать информационные характеристики дискретных источников сообщений и каналов связи; сжимать данные по методам Шеннона-Фано, Хаффмана, арифметического кодирования, Лемпела-Зива; защищать передаваемую информацию с помощью симметричных алгоритмов шифрования.

Владеть навыками построения и декодирования линейных блоковых кодов; навыками шифрования сообщений; навыками расчета энтропии дискретных источников сообщений; навыками расчета пропускной способности каналов связи.

2 Место дисциплины "Теория информации, данные, знания" в структуре ОПОП бакалавриата

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Дополнительные главы математики, Информатика, Информационные технологии, История информатики, Математика, Математическая логика и теория алгоритмов, Теория информационных процессов и систем, Физика.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Теория информации, данные, знания" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Теория информации, данные, знания" составляет 4 зачетных единицы, 144 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 2/Семестр 4			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия	32		
Практические занятия			

1621832750

Форма обучения	Количество часов		
	ОФ	**ЗФ**	**ОЗФ**
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа	60		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Теория информации, данные, знания", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Раздел 1. Теория информации как наука. Источники сообщений.			
Лекция 1.1. Предмет теории информации. Объем работы и формы контроля. Цель и задачи курса. Связь курса с другими дисциплинами. Сведения из истории развития теории информации. Предметная область теории информации, ее связь с другими науками. Понятие неопределенности и информации. Понятие сигнала, сообщения и данных. Система передачи сообщений и ее основные элементы.	2		
Лекция 1.2. Информационные характеристики источников сообщений. Энтропия дискретного источника сообщений без памяти. Формула Шеннона. Условная энтропия и ее свойства. Энтропия объединения и ее свойства. Взаимная информация и ее свойства. Избыточность, эффективность и производительность источника сообщений.	2		
Раздел 2. Эффективное и помехоустойчивое кодирование информации.			
Лекция 2.3. Особенности эффективного кодирования. Виды и характеристики кодов. Кодовые деревья. Неравенство Крафта. Понятие эффективного кодирования. Теорема Шеннона о кодировании источников. Методы сжатия информации.	2		
Лекция 2.4. Особенности помехоустойчивого кодирования Блоковые корректирующие коды. Понятие помехоустойчивого кодирования. Классификация помехоустойчивых кодов. Особенности и характеристики блоковых корректирующих кодов.	2		
Лекция 2.5. Линейные блоковые коды и их математическое описание. Основные понятия линейной алгебры. Математическое описание линейных блоковых кодов. Пространство Хэмминга. Границы для параметров линейных блоковых кодов.	2		
Лекция 2.6. Циклические коды, их математическое описание и построение. Понятие циклического кода. Полиномы и операции над ними. Построение циклических кодов. Порождающие полиномы. Линейные переключательные схемы циклических кодов.	2		
Раздел 3. Криптографическая защита информации			
Лекция 3.7. Предмет и основные понятия криптографии. Методы защиты секретной информации. Предмет и задачи криптографии. Основные понятия криптографии. Элементы системы передачи секретной информации. Этапы развития криптографии.	2		

1621832750

Лекция 3.8. Блочные алгоритмы шифрования. Особенности алгоритма DES. Блочные алгоритмы шифрования. Сеть Фейстеля. Особенности блочного алгоритма шифрования DES. Режимы работы алгоритма DES. Понятие об алгоритмах 3DES и Rijndael (AES).	2		
Итого	**16**		

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
1. Основы моделирования случайных величин и процессов	4		
2. Моделирование и расчет характеристик дискретных источников сообщений	4		
3. Моделирование и расчет характеристик дискретных каналов связи	4		
4. Сжатие информации методом арифметического кодирования	4		
5. Сжатие информации с помощью алгоритмов Лемпела-Зива	4		
6. Основы построения и декодирования линейных блоковых кодов	4		
7. Построение и декодирование циклических кодов	4		
8. Криптографическая защита информации с помощью симметричных алгоритмов шифрования	4		
Итого	**32**		

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	Трудоемкость в часах		
	ОФ	ЗФ	ОЗФ
Работа с конспектом лекций	10		
Оформление отчетов по лабораторным работам	16		
Самостоятельное изучение отдельных тем разделов дисциплины	16		
Самостоятельное выполнение практических заданий	18		
Итого	**60**		
Экзамен	**36**		

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Теория информации, данные, знания"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень
Контрольная работа, подготовка отчетов и оветы на контрольные вопросы по лабораторным занятиям, тестирование	ПК-3 - Оптимизация функционирования прикладного программного обеспечения	Выполняет построение и декодирование линей ных блоковых кодов. Выполняет расчёт информационных характеристик дискретных сообщений и пропускной способности каналов связи. Проводит сжатие данных различными методами. Проводит шифрование сообщений.	**Знать:** основные понятия теории информации; информационные характеристики источников сообщений и каналов связи и способы их оценки; основные методы эффективного (оптимального) кодирования и сжатия информации; основные виды помехоустойчивых кодов, методы их построения и декодирования; основные теоремы теории информации; основные понятия криптографии и методы шифрования информации. **Уметь:** строить и декодировать линейные блоковые коды для обнаружения и исправления ошибок в сообщениях; определять количество информации в дискретных сообщениях; рассчитывать информационные характеристики дискретных источников сообщений и каналов связи; сжимать данные по методам Шеннона-Фано, Хаффмана, арифметического кодирования, Лемпела-Зива; защищать передаваемую информацию с помощью симметричных алгоритмов шифрования. **Владеть:** навыками построения и декодирования линейных блоковых кодов; навыками шифрования сообщений; навыками расчета энтропии дискретных источников сообщений; навыками расчета пропускной способности каналов связи.	Высокий или средний

1621832750

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции -** компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции -** компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Контрольные задания или иные материалы

Ткущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ.

5.2.1.Оценочные средства при текущем контроле

Контрольные работы

При проведении контрольной работы обучающимся будет письменно, выдано задание, включающее теоретические и практические вопросы, на которые они должны дать ответы.

Критерии оценивания:

- 90 – 100 баллов – при правильном и полном ответе на два вопроса;

- 80 – 89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60 – 79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0 – 59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0 - 59	60 - 79	80 - 89	90 - 100
Шкала оценивания	неудовл	удовл	хорошо	отлично

Примерный перечень заданий для контрольных работ по разделам

Раздел 1. Теория информации как наука. Источники сообщений.

1. Что характеризует энтропия H дискретного источника сообщений без памяти, и в каком случае она максимальна?

2. Что характеризует и как определяется взаимная информация I(X,Y) статистически связанных источников сообщений X и Y?

3. Для источника сообщений без памяти, задаваемого ансамблем A требуется определить энтропию, а также среднее количество информации в сообщении a, получаемом от источника A.

4. Требуется определить условную энтропию H(B|A) источника B = {b1 , b2} относительно источника A (модель из задачи 3) и энтропию объединения H(A,B) источников A и B. Статистическая зависимость состояний источника B относительно состояний источника A задана матрицей P(a|b) переходных вероятностей.

5. Какие каналы связи называют стационарными каналами?

6. Каково необходимое и достаточное условие для того, чтобы код был префиксным?

7. Как при декодировании арифметического кода определяют очередной символ источника сообщений?

8. Определить пропускную способность дискретного канала связи без памяти при известном среднем времени τср передачи одного символа. Модель канала связи задана с помощью входного ансамбля X и матрицы переходных вероятностей P(Y | X).

9. Что называют дискретным источником сообщений?

10. Какие дискретные источники сообщений называют источниками без памяти?

11. Как между собой связаны вероятность единичного события и количество информации, получаемое от осуществления этого события?

12. Что характеризует энтропия дискретного источника сообщений?

13. Каким образом энтропия может быть определена для дискретного источника сообщений?

14. Как можно найти количество информации, содержащееся в дискретном сообщении?

15. В каком случае формула Хартли применима для определения количества информации в сообщении?

16. При каких условиях энтропия дискретного источника сообщений равна нулю?

17. В каком случае энтропия дискретного источника сообщений максимальна?

18. В чем заключается сущность эффективного кодирования?

19. Каковы основные задачи эффективного кодирования?

20. Как определяется средняя длина кодового слова?

21. Чему равна нижняя граница эффективного кодирования?

22. Как определяется эффективность и избыточность кода?

Раздел 2. Эффективное и помехоустойчивое кодирование информации.

1. Для источника без памяти, заданного ансамблем S, требуется построить код Хаффмана и соответствующее ему кодовое дерево. Определить эффективность и избыточность полученного кода.

2. Какие помехоустойчивые коды называют систематическими?

3. Как с помощью порождающей матрицей линейного блокового кода осуществляется кодирование информационных слов?

4. Для заданного блокового корректирующего кода требуется определить расстояние Хэмминга между первым и вторым кодовыми словами, определить кодовое расстояние и максимальное число ошибок, которое код может обнаружить и исправить. C = {000011, 110000, 010101, 101010}.

5. Используя код Хэмминга, для заданного информационного слова получить кодовое слово. Задать одиночную ошибку в кодовом слове и при декодировании произвести исправление этой ошибки. 0110011.

6. Что понимают под синдромом при декодировании линейных блоковых кодов?

7. В чём заключается основное свойство циклических кодов, давшее им название «циклические» коды?

8. Выполнить кодирование информационного вектора v с помощью циклического (7, 4)-кода, задаваемого порождающим полиномом G3 (x) = x 3 + x 2 + 1. Задать в полученном кодовом полиноме одиночную ошибку и произвести её исправление при декодировании. v = 1010.

9. В чем заключается сущность эффективного кодирования?

10. Каковы основные задачи эффективного кодирования?

11. Как определяется средняя длина кодового слова?

12. Чему равна нижняя граница эффективного кодирования?

13. Как определяется эффективность и избыточность кода?

14. Как осуществляется кодирование источника по методу Шеннона-Фано?

15. В каком случае метод Шеннона-Фано гарантированно обеспечивает получение эффективного кода?

16. С помощью какой операции в методе Хаффмана обеспечивается получение вспомогательных символов?

17. Какие помехоустойчивые коды называют блоковыми?

18. Что такое расстояние Хэмминга?

19. Что называют кодовым расстоянием?

20. Какие коды называют линейными блоковыми?

21. Как определяется кодовое расстояние для линейного блокового кода?

22. Какие коды называют систематическими?

23. Сколько ошибок способен обнаруживать и исправлять код Хэмминга?

24. По какому правилу определяют число проверочных символов в коде Хэмминга?

25. В каких местах располагаются проверочные символы в кодовых словах Хэмминга?

26. По какому правилу строятся уравнения для нахождения проверочных символов в коде Хэмминга?

27. Какую информацию при декодировании кода Хэмминга дает синдром?

28. Каким образом обеспечивается обнаружение двойных ошибок в расширенном коде Хэмминга?

Раздел 3. Криптографическая защита информации.

1. Что означает требование обратимости преобразования при шифровании и расшифровании?

2. Зашифровать сообщение методом столбцовой перестановки по таблице 4 × 4. Ключ указывает порядок считывания текста по столбцам при шифровании. С помощью этого же ключа расшифровать заданный шифротекст. Ключ: (2, 1, 3, 4) Шифротекст: АА_ЕЗЧЕШАНЕАД_РН.

3. В чём заключается основное различие между симметричными и асимметричными алгоритмами шифрования?

4. Что называют шифром?

5. В чём заключается различие между расшифрованием и дешифрованием?

6. Что понимают под ключом в криптографии?

7. Какие шифры называют шифрами перестановки?

8. В чём заключается шифрование перестановкой с фиксированным периодом?

1621832750

9. Какие шифры называют шифрами замены?

10. Как осуществляется шифрование в шифре Цезаря?

11. Каким образом можно определить ключ для шифра сдвига?

12. Что понимают под шифрами простой замены?

13. Как можно осуществить взлом шифра простой замены?

14. В чём заключаются особенности шифра Виженера?

Отчеты по лабораторным занятиям

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных занятий п.4 рабочей программы).

Содержание отчета:

1. Тема лабораторного занятия.

2. Задачи лабораторного занятия.

3. Краткое описание хода выполнения.

4. Ответы на задания или полученные результаты по окончании выполнения (в зависимости от задач, поставленных в п. 2).

5. Выводы.

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме;

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0 –59	60 – 100
Шкала оценивания	не зачтено	зачтено

Опрос по контрольным вопросам к лабораторным работам

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Критерии оценивания:

- 90 – 100 баллов – при правильном и полном ответе на два вопроса;

- 80 – 89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60 – 79 баллов – при правильном и полном ответе только на один из вопросов или приправильном, но не полном ответе на два вопроса;

- 0 – 59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0 - 59	60 - 79	80 - 89	90 - 100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов по лабораторным занятиям (работам)

Раздел 1. Теория информации как наука. Источники сообщений.

Лабораторная работа "Основы моделирования случайных величин и процессов"

1. Что понимают под случайной величиной?

2. Что называют функцией распределения?

3. Что такое ансамбль дискретной случайной величины?

Лабораторная работа "Моделирование и расчет характеристик дискретных источников сообщений"

1. Что понимают под дискретным источником сообщений?

2. Какие дискретные источники сообщений называют источниками с памятью?

3. Что понимают под цепью Маркова?

Лабораторная работа "Моделирование и расчет характеристик дискретных каналов связи"

1. Что понимают под каналом связи?

2. Какие каналы связи называют дискретными?

3. Что понимают под дискретным каналом без памяти?

Раздел 2. Эффективное и помехоустойчивое кодирование информации.

Лабораторная работа "Сжатие информации методом арифметического кодирования"

1. Что понимают под сжатием информации?

2. В какую форму преобразуется последовательность символов в методе арифметического кодирования?

3. Что понимают под кумулятивными вероятностями символов?

Лабораторная работа "Сжатие информации с помощью алгоритмов Лемпела-Зива"

1. В чём заключаются основные особенности словарных методов сжатия информации?

2. Какие виды словарей применяются в словарных методах сжатия?

3. На какие группы разделяют семейство алгоритмов Лемпела-Зива?

Лабораторная работа "Основы построения и декодирования линейных блоковых кодов"

1. Какие помехоустойчивые коды называют блоковыми?

2. Что такое расстояние Хэмминга?

3. Что называют кодовым расстоянием?

Лабораторная работа "Построение и декодирование циклических кодов"

1. В чем заключаются основные особенности циклических кодов?

2. Какие полиномы называют неприводимыми в поле GF(q)?

3. Что понимают под порождающими полиномами циклических кодов?

Раздел 3. Криптографическая защита информации.

Лабораторная работа "Криптографическая защита информации с помощью симметричных алгоритмов шифрования"

1. Какие шифры называют симметричными?

2. В чём заключается различие между блочными и поточными алгоритмами шифрования?

3. Что понимают под рассеиванием и перемешиванием в блочных шифрах?

Тестирование

При проведении текущего контроля обучающимся необходимо ответить на тестирование по каждому разделу. Тестирование может быть организовано с использованием ресурсов ЭИОС КузГТУ.

Критерии оценивания:

- 60 – 100 баллов – при ответе на не менее 60% вопросов;
- 0 – 59 баллов – при ответе на менее 60% вопросов.

Количество баллов	0–59	60–100
Шкала оценивания	не зачтено	зачтено

Примеры тестовых вопросов

Раздел 1. Теория информации как наука. Источники сообщений.

1. Вопрос: Источник сообщения, который может в каждый момент времени случайным образом принять одно из конечного множества возможных состояний, называется?

варианты ответов: Источник с памятью; Источник без памяти; Дискретным источником; Марковским источником.

2. Вопрос: В технике под информацией понимают?

варианты ответов: Воспринимаемые человеком или специальными устройствами сведения об окружающем мире и протекающих в нем процессах; Часть знаний, использующихся для ориентирования, активного действия, управления; Сообщения, передающиеся в форме знаков или сигналов; Сведения, обладающие новизной.

3. Вопрос: Примером числовой информации может служить:

варианты ответов: Разговор по телефону; Иллюстрация в книге; Таблица значений тригонометрических функций; Симфония.

Раздел 2. Эффективное и помехоустойчивое кодирование информации.

1. Вопрос: В какой кодовой таблице можно закодировать 65536 различных символов?

варианты ответов: CP-1251; ASCII; Unicode; КОИ-8Р.

2. Вопрос: При блочном кодировании информация делится на?

варианты ответов: Блоки определенной длины; Группы определенной длины; Источники определенной длины; Блоки неопределенной длины.

3. Вопрос: Не избыточным помехоустойчивым кодированием является?

варианты ответов: Декодирование; Сжатие информации; Цифро-аналоговое преобразование; Скремблирование.

Раздел 3. Криптографическая защита информации.

1. Вопрос: Разработкой методов шифрования данных занимается?

варианты ответов: Криптование; Криптография; Криптоанализ; Криптология.

2. Вопрос: Что такое криптография?

варианты ответов: Кодирование информации с целью защиты от несанкционированного доступа; Кодирование информации с целью устранения помех; Кодирование информации с целью исправления ошибок; Кодирование информации с целью выявление помех.

3. Вопрос: Является полиграммным шифром, который может использовать большие группы с помощью линейной алгебры. Каждой букве сперва сопоставляется число. Это шифр …

варианты ответов: Хилла; Хэмминга; Альберти; Плейфера; Уитстона.

Полный перечень вопросов для текущего тестирования представлен в ЭИОС КузГТУ и системе

Moodle.

5.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является зачет/экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты и ответы на контрольные вопросы обучающихся по лабораторным занятиям;
- ответы обучающихся на тестовые вопросы.

При проведении промежуточного контроля обучающийся отвечает на 2 теоретических вопроса выбранных случайным образом и решает одну задачу или на 15 вопросовв в тестировании. Опрос может проводиться в письменной и (или) устной, и (или) электронной форме.

Ответы на вопросы

Критерии оценивания при ответе на вопросы:

- 90 – 100 баллов – при правильном и полном ответе на два вопроса и решении практической задачи;
- 80 – 89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов и решении практической задачи;
- 60 – 79 баллов – при правильном и неполном ответе только на два вопроса;
- 0 – 59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0 - 59	60 - 79	80 - 89	90 - 100
Шкала оценивания	неуд	удовл	хорошо	отлично
	не зачтено		зачтено	

Примерный перечень вопросов к экзамену

Теоретические вопросы

1. Предметная область теории информации, ее связь с другими науками.
2. Понятия информации и неопределенности. Понятия сигнала, сообщения и данных.
3. Система передачи информации, ее основные элементы.
4. Количественная оценка информации. Количество информации и вероятность.
5. Энтропия дискретного источника сообщений без памяти. Формула Шеннона.
6. Математические свойства энтропии дискретных сообщений.
7. Понятие о цепях Маркова. Марковские источники сообщений.
8. Статистически связанные источники. Условная энтропия и ее свойства.
9. Объединение источников. Энтропия объединения и ее свойства.
10. Взаимная информация и ее свойства.
11. Эффективность, избыточность и производительность источников сообщений.
12. Виды каналов связи. Дискретные каналы связи без памяти.
13. Пропускная способность дискретного канала связи без памяти.
14. Равномерные и неравномерные коды. Кодовые деревья. Неравенство Крафта.
15. Эффективное кодирование. Теорема Шеннона о кодировании источников.
16. Классификация методов сжатия информации.
17. Метод Шеннона-Фано.
18. Метод Хаффмана.
19. Метод арифметического кодирования.
20. Словарные методы сжатия информации. Метод RLE.
21. Особенности алгоритма LZ77.
22. Особенности алгоритма LZ78.
23. Помехоустойчивое кодирование. Теорема Шеннона о кодировании каналов.
24. Классификация помехоустойчивых кодов.
25. Особенности и характеристики блоковых корректирующих кодов.
26. Математическое описание линейных блоковых кодов.
27. Систематические коды. Код Хэмминга.
28. Порождающие матрицы линейных блоковых кодов.
29. Проверочные матрицы линейных блоковых кодов.
30. Декодирование линейных блоковых кодов.
31. Понятие циклического кода. Полиномы и операции над ними.
32. Построение циклических кодов. Порождающие полиномы.
33. Проверочные полиномы. Декодирование циклических кодов.
34. Методы защиты секретной информации. Предмет и задачи криптографии.
35. Основные понятия криптографии.

36. Формальные модели шифров.
37. Классификация симметричных шифров.
38. Многоалфавитные шифры замены. Шифр Виженера.
39. Классификация современных криптографических алгоритмов.
40. Блочные алгоритмы шифрования. Сеть Фейстеля.
41. Особенности блочного алгоритма DES.
42. Режимы работы алгоритма DES.
43. Правило Керкгоффа. Виды атак на шифр.
44. Расстояние единственности.
45. Абсолютно стойкий шифр.

Практические задания

1. Определить пропускную способность дискретного канала связи, заданного матрицей переходных вероятностей P(b|a). Каждый символ вырабатывается источником сообщений за 0,01 сек. Найти информационные потери при передаче через заданный канал 100 символов.

2. Произвести эффективное кодирование алфавита источника сообщений, задаваемого ансамблем S, с помощью метода Хаффмана. Построить кодовое дерево для полученного кода Хаффмана и определить его эффективность.

3. Перекодировать информационный вектор в код Хэмминга. Задать одиночную ошибку в полученном кодовом векторе Хэмминга и произвести его декодирование по синдрому, исправив эту ошибку. Получить расширенный код Хэмминга, задать в нем двойную ошибку и обнаружить ее при декодировании.

Тестирование

При проведении текущего контроля обучающимся необходимо ответить на тестирования по каждому разделу. Тестирование может быть организовано с использованием ресурсов ЭИОС КузГТУ.

Критерии оценивания:

- 90 – 100 баллов – при ответе на не менее 90% вопросов;
- 80 – 89 баллов – при ответе на более 79% и менее 90% вопросов;
- 60 – 79 баллов – при ответе на более 59% и менее 80% вопросов;
- 0 – 59 баллов – при ответе менее 60% вопросов.

Количество баллов	0 - 59	60 - 79	80 - 89	90 - 100
Шкала оценивания	неудовл	удовл	хорошо	отлично
	не зачтено		зачтено	

Примеры тестовых вопросов

Раздел 1. Теория информации как наука. Источники сообщений.

1. Вопрос: Источник сообщения, который может в каждый момент времени случайным образом принять одно из конечного множества возможных состояний, называется?

варианты ответов: Источник с памятью; Источник без памяти; Дискретным источником; Марковским источником.

2. Вопрос: В технике под информацией понимают?

варианты ответов: Воспринимаемые человеком или специальными устройствами сведения об окружающем мире и протекающих в нем процессах; Часть знаний, использующихся для ориентирования, активного действия, управления; Сообщения, передающиеся в форме знаков или сигналов; Сведения, обладающие новизной.

3. Вопрос: Примером числовой информации может служить:

варианты ответов: Разговор по телефону; Иллюстрация в книге; Таблица значений тригонометрических функций; Симфония.

Раздел 2. Эффективное и помехоустойчивое кодирование информации.

1. Вопрос: В какой кодовой таблице можно закодировать 65536 различных символов?

варианты ответов: CP-1251; ASCII; Unicode; КОИ-8Р.

2. Вопрос: При блочном кодировании информация делится на?

варианты ответов: Блоки определенной длины; Группы определенной длины; Источники определенной длины; Блоки неопределенной длины.

3. Вопрос: Не избыточным помехоустойчивым кодированием является?

варианты ответов: Декодирование; Сжатие информации; Цифро-аналоговое преобразование; Скремблирование.

Раздел 3. Криптографическая защита информации.

1. Вопрос: Разработкой методов шифрования данных занимается?

варианты ответов: Криптование; Криптография; Криптоанализ; Криптология.

1621832750

2. Вопрос: Что такое криптография?

варианты ответов: Кодирование информации с целью защиты от несанкционированного доступа; Кодирование информации с целью устранения помех; Кодирование информации с целью исправления ошибок; Кодирование информации с целью выявление помех.

3. Вопрос: Является полиграммным шифром, который может использовать большие группы с помощью линейной алгебры. Каждой букве сперва сопоставляется число. Это шифр …

варианты ответов: Хилла; Хэмминга; Альберти; Плейфера; Уитстона.

Полный перечень вопросов для текущего тестирования представлен в ЭИОС КузГТУ и системе Moodle.

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник выдаёт вариант контрольной работы.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторной работы осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе и ответе на два контрольный вопроса, которые задаются в устной или письменной форме. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

2. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два теоретических вопроса и одно практическое задание, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Лихачева, Г. Н. Информационные системы и технологии / Г. Н. Лихачева, М. С. Гаспариан. – Москва : Евразийский открытый институт, 2011. – 370 с. – ISBN 9785374001921. – URL: http://biblioclub.ru/index.php?page=book_red&id=90543 (дата обращения: 27.06.2022). – Текст : электронный.

2. Турчин, Д. Е. Теория информации. Лабораторный практикум : учебное пособие : для студентов направления подготовки 09.03.02. «Информационные системы и технологии / Д. Е. Турчин ; Кузбасский государственный технический университет им. Т. Ф. Горбачева, Кафедра информационных и автоматизированных производственных систем. – Кемерово : КузГТУ, 2016. – 1 электрон. опт. диск (CD-ROM). – URL: http://library.kuzstu.ru/meto.php?n=91434&type=utchposob:common (дата обращения: 27.06.2022). – Текст : электронный.

3. Балюкевич, Э. Л. Теория информации / Э. Л. Балюкевич. – Москва : Евразийский открытый институт, 2009. – 215 с. – ISBN 9785374002195. – URL: http://biblioclub.ru/index.php?page=book_red&id=90441 (дата обращения: 27.06.2022). – Текст : электронный.

6.2 Дополнительная литература

1. Назаров, С. В. Современные операционные системы / С. В. Назаров, А. И. Широков. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ),Бином. Лаборатория знаний, 2011. – 280 с. – ISBN 9785996304165. – URL: http://biblioclub.ru/index.php?page=book_red&id=233197 (дата обращения: 27.06.2022). – Текст : электронный.

2. Романов, В. П. Интеллектуальные информационные системы в экономике : учеб. пособие для студентов вузов, обучающихся по специальности "Прикладная информатика" / под ред. Н. П. Тихомирова; Рос. экон. акад. им. Г. В. Плеханова. – М. : ЭКЗАМЕН, 2003. – 496 с. – Текст : непосредственный.

3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2012. – 592 с. – ISBN 9785940746379. – URL: http://biblioclub.ru/index.php?page=book_red&id=231889 (дата обращения: 27.06.2022). – Текст : электронный.

4. Турчин, Д. Е. Теория информации : методические указания к лабораторным работам для студентов направления подготовки 230400.62 «Информационные системы и технологии» очной формы обучения / Д. Е. Турчин ; ФГБОУ ВПО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. информ. и автоматизир. произв. систем. – Кемерово : КузГТУ, 2014. – 150с. – URL: http://library.kuzstu.ru/meto.php?n=8129 (дата обращения: 27.06.2022). – Текст : электронный.

5. Иванова, С. М. Теория информации. Моделирование интеллектуальных систем : учебное пособие / С. М. Иванова, З. В. Ильиченкова. — Москва : РТУ МИРЭА, 2020. — 65 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163804 (дата обращения: 27.06.2022). — Режим доступа: для авториз. пользователей.

1621832750

6.3 Методическая литература

1. Теория информации : методические указания к самостоятельной работе для студентов направления подготовки 09.03.02 «Информационные системы и технологии» очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. и автоматизир. произв. систем ; сост. Д. Е. Турчин. – Кемерово : КузГТУ, 2016. – 144 с. – URL: http://library.kuzstu.ru/meto.php?n=4504 (дата обращения: 27.06.2022). – Текст : электронный.

2. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И. Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: http://library.kuzstu.ru/meto.php?n=553 (дата обращения: 27.06.2022). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://elib.kuzstu.ru/index.php?option=com_content&view=article&id=230&Itemid=229
4. Электронная библиотечная система Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
6. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Вестник Кузбасского государственного технического университета : научно-технический журнал (печатный/электронный) https://vestnik.kuzstu.ru/
2. Информационные системы и технологии : научно-технический журнал (электронный) https://elibrary.ru/contents.asp?titleid=28336
3. Информационные технологии и вычислительные системы : журнал (печатный/электронный) https://elibrary.ru/contents.asp?titleid=8746
4. Информация и безопасность : научный журнал (печатный)
5. Открытые системы. СУБД : журнал (печатный/электронный) https://elibrary.ru/contents.asp?titleid=9826
6. Прикладная информатика : научно-практический журнал (электронный) https://elibrary.ru/contents.asp?titleid=25599
7. Программные продукты и системы : международный научно-практический журнал (печатный)

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Теория информации, данные, знания"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Теория информации, данные, знания", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. Opera
5. Yandex
6. Open Office
7. Microsoft Windows

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Теория информации, данные, знания"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.