

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 08.11.2023 10:03:05
Уникальный программный ключ:
69e375c64f7e975d4e8850e7b4fcc2ad0bf35f08

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семькина

« 4 » 09



Рабочая программа дисциплины (с аннотацией)

Теория кодирования, сжатия и восстановления информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:

Семькина Н. А.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области применения и построения алгоритмов кодирования, сжатия и восстановления информации, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

- 1) получение базовых знаний и умений, связанных с основными понятиями теории кодирования, сжатия и восстановления информации;
- 2) формирование навыков и умения применять различные методы и алгоритмы кодирования, сжатия и восстановления информации.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Теория информации», «Алгебра», «Дискретная математика», «Математическая логика и теория алгоритмов».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Математические методы обработки сигналов», «Теория вычислительной сложности», «Аналитика больших данных», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 30 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 30 часов, в т.ч. практическая подготовка – 7 часа;

самостоятельная работа: 48 часа.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1 Производит стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ
	ОПК-3.2 Решает основные задачи линейной алгебры и аналитической геометрии
	ОПК-3.5 Оценивает сложность алгоритмов и вычислений
	ОПК-3.6 Применяет методы математической логики и теории алгоритмов к решению задач математической кибернетики

	ОПК-3.9 Применяет стандартные методы дискретной математики для решения профессиональных задач
	ОПК-3.14 Разрабатывает вероятностные и статистические модели при решении типовых прикладных задач
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1 Применяет основы теории чисел в криптографии и других дисциплинах
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.3 Решает типовые задачи кодирования и декодирования
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	ОПК-2.1.1. Использует в профессиональной деятельности криптографические алгоритмы и реализует их программно
	ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации
ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации	ОПК-2.2.1. Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы
	ОПК-2.2.2. Разрабатывает математические модели, реализуемые в средствах защиты информации
ОПК-2.3. Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов	ОПК-2.3.1 Применяет национальные, межгосударственные и международные стандарты в области защиты информации
	ОПК-2.3.2 Анализирует существующие методы и средства, применяемые для контроля и защиты информации

5. Форма промежуточной аттестации и семестр прохождения – зачет в 8 семестре.

6. Язык преподавания русский.

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
1 Раздел Теория кодирования	50	14	12	3	21
Основные понятия и задачи теории кодирования. Математическая постановка задачи. Помехоустойчивое кодирование.	5	2	1	0	2
Алфавитное неравномерное двоичное кодирование. Префиксный код	6	2	2	0	2
Линейные коды	7	2	2		3
Декодирование линейных кодов	8	2	2	1	3
Циклические коды	8	2	2	1	3
Декодирование циклического кода	9	2	2	1	4
Мажоритарное кодирование	7	2	1	0	4
2 Раздел Теория сжатия и восстановления информации	58	16	11	4	27
Сжатие информации. Технические характеристики процесса сжатия данных. Простейшие методы сжатия информации	8	2	2	0	4
Универсальные методы сжатия	10	2	2	2	4
LZW - кодирование	10	2	2	2	4
Сжатие текстовой информации	7	2	2	0	3

Сжатие графической информации	8	3	1	0	4
Сжатие аудиоданных	8	3	1	0	4
Сжатие видеоданных	7	2	1	0	4
ИТОГО	108	30	23	7	48

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
1 Раздел. Теория кодирования	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
2 Раздел. Теория сжатия и восстановления информации	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения текущей аттестации

Задания для практических (семинарских) занятий

1 Раздел.

Задание 1 (ОПК-3.1, ОПК-3.2, ОПК-3.5, ОПК-3.6, ОПК-10.3): . Код C над полем F_2 задан порождающей матрицей:

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

Определить основные параметры эквивалентного систематического кода и декодировать слово 0101.

Задание 2 (ОПК-3.1, ОПК-3.2, ОПК-3.5, ОПК-3.6, ОПК-10.3): Для линейного кода, заданного порождающей матрицей

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

построить таблицу стандартного расположения. Декодировать слово (1 1 0 1 1 1) по таблице стандартного расположения и слово (1 0 1 0 1 1) с помощью синдрома.

Задание 3 (ОПК-3.6, ОПК-3.14, ОПК-10.3): Построить коды Шеннона - Фано и Хаффмена найти стоимости кодирований для источников Бернулли с вероятностями букв:

$$P = \{0.5; 0.2; 0.1; 0.09; 0.08; 0.03\}.$$

Задание 4 (ОПК-8.1, ОПК-10.3): Дан циклический код длины 15 с

порождающим многочленом

$$g(x) = (x^3+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Выполнить кодирование $m(x)=(1010111)$ для систематического и несистематического кода.

2 Раздел.

Задание 1 (ОПК-2.1.1, ОПК-2.1.2, ОПК-2.2.1, ОПК-2.2.2): Пусть дан монотонный источник $A = \{a, b, c, d\}$. Передать слово $w = cbbaccddbb$ с помощью кода «стопка книг». Декодировать полученное слово.

Задание 2 (ОПК-2.1.1, ОПК-2.1.2, ОПК-2.2.1, ОПК-2.2.2): Закодировать строку методом Лемпеля-Зива – Велча

WECANNOTWEWOULDWECANWECAN #

Задание 3 (ОПК-2.2.1, ОПК-2.2.2, ОПК-2.3.1, ОПК-2.3.2): Выполнить сжатие сообщения методом RLE. С помощью таблицы CP-1251 перевести символы заданной фразы в десятичные числа, а затем десятичные числа перевести в двоичные.

Текст сообщения: КОД 377hhhs4444555.

Задание 4 (ОПК-2.2.1, ОПК-2.2.2, ОПК-2.3.1, ОПК-2.3.2): Известен блок P изображения размера 4×4 . Выполните для него дискретное косинусное преобразование.

Оценочные материалы для проведения промежуточной аттестации

Проверяемые индикаторы достижения компетенций: ОПК-3.1; ОПК-3.2; ОПК-3.5; ОПК-3.6; ОПК-3.9; ОПК-3.14; ОПК-8.1; ОПК-10.3; ОПК-2.1.1; ОПК-2.1.2; ОПК-2.2.1; ОПК-2.2.2; ОПК-2.3.1; ОПК-2.3.2.

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к зачету

1. Основные понятия и задачи теории кодирования. Математическая постановка задачи.
2. Первая теорема Шеннона. Кодирование сигнала. Способы кодирования/ декодирования информации.
3. Двоичное кодирование. Алфавитное неравномерное двоичное кодирование (метод Шеннона-Фано, метод Хаффмена).
4. Линейный код. Задание кода. Теорема о связи проверочной и порождающей матриц. Определение синдрома.
5. Декодирование линейных кодов. Типы декодирования. Синдромное декодирование.
6. Декодирование линейных кодов. Типы декодирования. Декодирование по максимуму правдоподобия (декодирование по лидеру смежного класса).
7. Декодирование по информационным совокупностям. Вероятность ошибки декодирования.
8. Циклический код. Теорема существования. Порождающая и проверочная матрицы. Систематические кодеры.
9. Декодирование циклического кода. Прямой метод декодирования.
10. Декодирование циклического кода. Синдромное декодирование. Общий алгоритм обнаружения и исправления ошибок.
11. Дуальные коды. Код Адамара, код Рида - Маллера

12. Сжатие информации. Технические характеристики процесса сжатия данных. Простейшие методы сжатия информации.
13. Сжатие информации. Технические характеристики процесса сжатия данных. Метод Г. В. Лавинского.
14. Универсальные методы сжатия информации. Классы методов сжатия. Арифметическое кодирование.
15. Универсальные методы сжатия информации. Классы методов сжатия. Сжатие способом кодирования серий последовательностей (Run Length Encoding - RLE)
17. Сжатие информации. Семейство алгоритмов Лемпеля-Зива.
18. Сжатие информации. Алгоритм Лемпеля-Зива – Велча.
19. Сжатие графических файлов.
20. Сжатие аудиоданных.
21. Сжатие видеоданных

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – 3 балла. Для получения зачета необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 2-х баллов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Кутликова И. В. Представление и кодирование информации. Логические основы обработки информации [Электронный ресурс] : учебно-методическое пособие / И. В. Кутликова, И. А. Черенкова, М. В. Новиков. - Москва : МГАВМиБ им. К.И. Скрябина, 2022. - 99 с. – Режим доступа: <https://e.lanbook.com/book/331364>

Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7 [Электронный ресурс]. – Режим доступа: <http://znanium.com/go.php?id=544713>

б) Дополнительная литература:

Кутликова И. В. Информация и информационные процессы. Представление и кодирование информации [Электронный ресурс] : методические рекомендации / И. В. Кутликова, И. А. Черенкова. - Москва : МГАВМиБ им. К.И. Скрябина, 2021. - 56 с. – Режим доступа: <https://e.lanbook.com/book/196238>

Сальникова Н.А. Информатика. Основы информатики. Представление и кодирование информации. Часть 1 [Электронный ресурс]: учебное пособие/ Н.А. Сальникова.— Электрон. текстовые данные.— Волгоград: Волгоградский институт бизнеса, Вузовское образование, 2009.— 94 с.— Режим доступа: <http://www.iprbookshop.ru/11321.html>

2) Программное обеспечение

Adobe Acrobat Reader DC - Russian	бесплатно Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Cadence SPB/OrCAD 16.6	103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011; Акт предоставления прав № Us000311 от 25.09.2012;
MATLAB R2012b	
Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
МиKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань <https://e.lanbook.com/> Договор № 4-е/23 от 02.08.2023 г.

2. ЭБС Znanium.com <https://znanium.com/> Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online <https://biblioclub.ru> Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ <https://urait.ru/> Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART <https://www.iprbookshop.ru/> Договор № 3-е/23К от 02.08.2023 г.
6. <https://cyberleninka.ru/> научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозиторий ТвГУ <http://eprints.tversu.ru>

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. Библиотека сетевой безопасности <https://www.opennet.ru/links/info/297.shtml?skip=0>

VI. Методические материалы для обучающихся по освоению дисциплины
Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	50	18	12	20
2	50	18	12	20

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:

<https://tversu.ru/sveden/files/204->

[R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf](#)

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
<p>Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория. Математический кабинет № 213 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)</p> <p>Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)</p> <p>Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 314</p>	<p>Столы, стулья, переносной ноутбук, проектор</p> <p>Столы, стулья, переносной ноутбук, проектор</p> <p>Столы, стулья, переносной ноутбук, проектор</p>	<p>Adobe Acrobat Reader DC - Russian-бесплатно; Cadence SPB/OrCAD 16.6-Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009; Git version 2.5.2.2-бесплатно; Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus 1.4.0-бесплатно; Mathcad 15 M010-Акт предоставления прав IC00000027 от 16.09.2011; MATLAB R2012b-Акт предоставления прав № Us000311 от 25.09.2012; Многофункциональный редактор ONLYOFFICE -бесплатно; ОС Linux Ubuntu бесплатное ПО-бесплатно; Microsoft Web Deploy 3.5-бесплатно; MiKTeX 2.9-бесплатно; MSXML 4.0 SP2 Parser and SDK-бесплатно; MySQL Workbench 6.3 CE-бесплатно; NetBeans IDE 8.0.2-бесплатно; Notepad++-бесплатно; Origin 8.1 Sr2-договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд» ; PostgreSQL 9.6 -бесплатно; Python 3.4.3-бесплатно; Visual Studio 2010 Prerequisites - English-Акт на передачу прав №785 от 06.08.2021 г. ; WCF RIA Services V1.0 SP2-бесплатно; WinDjView 2.1-бесплатно; WinPcap 4.1.3-бесплатно; Wireshark 2.0.0 (64-bit)-бесплатно; R studio-бесплатно.</p>

(Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2018
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021

8.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023
----	--	--	---------------------------