Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Теория кодирования

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

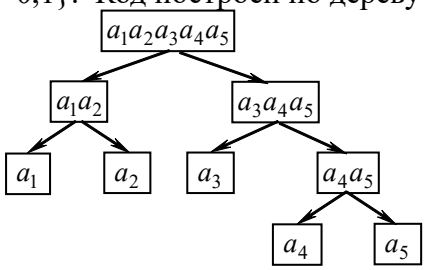
ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– тесты;
– индивидуальные задания, выполняемые на практических занятиях;
– контрольные работы

Тест (ИОПК-3.1)

1. Пусть A = {a_i} – кодируемый алфавит, p_i – частота символа a_i , a_i – кодируется словом B_i . Коэффициентом избыточности кода C = {B_i} называется величина:
   а) $\sum_{i \in C} p_i \cdot |B_i|$,
   б) $\min_{i \in C}(p_i \cdot |B_i|)$,
   в) $\max_{i \in C}(p_i \cdot |B_i|) \cdot$
2. Пусть A = {a_1, a_2, a_3, a_4, a_5 } и вероятности появления букв соответственно равны {0,3; 0,25; 0,2; 0,15; 0,1}. Код построен по дереву



   Какой алгоритм был использован для построения кодового дерева
   а) Алгоритм Фано;
   б) Алгоритм Хаффмана
3. Мощностью кода называется [вставить ответ] кода.
4. Укажите максимальное количество ошибок может исправить код, если его кодовое расстояние равно 8. (ввести ответ)
5. Какая из предложенных оценок параметров кода носит название границы Хемминга:
   а) $n - k \geq \log_2(1 + C_n^1 + C_n^2 + \ldots + C_n^{[(d-1)/2]})$,

б) $d_C \le \dfrac{n \cdot 2^{k-1}}{2^k - 1}$,

в) $d_C \le n - k + 1$;

г) $q^{n-k} > \sum_{j=0}^{d-2} C_{n-1}^{j} (q-1)^j$.

6. Является ли код {0000, 1010, 0101, 1111} линейным.
   а) да;
   б) нет.
7. Мощность двоичного линейного (n,k)-кода равна:
   а) 2^k;
   б) 2^n;
   в) 2^{n-k} .
8. Верно ли, что две матрицы G_1 и G_2 являются порождающими для одного и того же линейного кода, если

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

   а) да;
   б) нет.
9. Закодируйте информационное слово (1010) линейным (8,4)-кодом, с порождающей матрицей G и проверочной матрицей H, где

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

   (ввести ответ).
10. Имеется таблица декодирования для линейного кода C = {0000, 1001, 0110, 1111}. Верно ли утверждение, что эта таблица со стандартным расположением векторов

0000	1001	0110	1111
1000	0001	1110	0111
0100	1101	0010	1011
1100	0101	1010	0011

   а) да;
   б) нет

Ключи: 1 – а; 2 – а; 3 – количество слов ~ число слов; 4 – 3; 5 – а; 6 – а; 7 – а; 8 – а; 9 – 0101 1010; 10 – а.

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на половину вопросов (набрал не менее 2,5 балла). По итогу тестирования выставляются оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если результат тестирования – не менее 4,50 балла.

Оценка «хорошо» выставляется, если результат тестирования – от 3,50 до 4,49 баллов.

Оценка «удовлетворительно» выставляется, если результат тестирования – от 2,50 до 3,49 баллов.

Оценка «неудовлетворительно» выставляется, если тест не пройден (результат тестирования – менее 2,50 балла).

Индивидуальные задания, выполняемые на практических занятиях (ИОПК-3.2, ИОПК-3.3)

Каждое задание состоит из 1 – 3 задач, соответствующих теме занятия.

Занятие 1.

1. Выяснить, является ли кодирование φ однозначным. Если нет, то указать слово, декодируемое неоднозначно:

$\varphi(v_1) = ab$, $\varphi(v_2) = ba$, $\varphi(v_3) = cba$, $\varphi(v_4) = cab$, $\varphi(v_5) = acba$, $\varphi(v_6) = abbac$, $\varphi(v_7) = cccb$.

2. Построить схему оптимального префиксного алфавитного кодирования по методу Хаффмана для распределения вероятностей P появления букв алфавита

V = {a, b, c, d, e, f}

в сообщении при двоичном кодировании: P = {0,5; 0,2; 0,1; 0,09; 0,08; 0,03}. Найти коэффициент избыточности кода.

Занятие 3.

3. Найдите кодовое слово, в которое линейный (5,3)-код с порождающей матрицей $\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ кодирует информационное слово u=(011).

4. Найдите проверочную матрицу для линейного (5,3)-кода с порождающей матрицей $\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$. Проверить, являются ли кодовыми слова (101000) и (11111). Используя синдром, исправить ошибку в слове, не являющимся кодовым.

Занятие 5.

5. Закодировать (7,4)-кодом Хемминга сообщение (1101).

6. Восстановить кодовое слово, если кодирование было осуществлено (10,6)-кодом Хемминга и принято слово (1001 0110 11)

Занятие 6.

7. Декодировать слово u = (1001 1011 0010 0001), зная, что был использован RM(2,4) код.

Занятие 7.

8. Циклический (7,4) код порождается многочленом $g(x) = x^3 + x^2 + 1$. Дано двоичное представление слова «дача»:

(1010 0100 1010 0000 1110 01111 1010 0000)

(для двоичного представления слова «дача» использован ASCII-код). Закодируйте это слово.

Занятие 8.

9. Запишите порождающий многочлен кода БЧХ длины n=15, исправляющего 3 ошибки. Для построения поля $GF(2^4)$ используйте примитивный многочлен $x^4 + x^3 + 1$.

10. Исправить ошибки в слове (1101 0100 0011 101), если для кодирования использовался записанный порождающий многочлен, найденный вами в задаче 9.

Ответы:

Задача 1. Кодирование неоднозначное, abbacccbacba = $B_6B_3B_3 = B_1B_2B_7B_5$.

Задача 2. Код: {0, 11, 1000, 1001, 1010, 1011} коэффициент избыточности k = 2,1 .

Задача 3. 01111 .

Задача 4. $\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$, (101000) – кодовое слово, (11111) – не кодовое слово; синдром – 10 .

Задача 5. (1010 101)

Задача 6. Синдром (0111) ⇒ позиция ошибки k=7 ⇒ исправленное слово: (1001 0100 11) .

Задача 7. Информационное слово (1101 1001 101) .

Задача 8. Кодовое слово: (1000110 0110100 1000110 0000000 1001011 0100011 1000110 0000000) .

Задача 9. $(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$

Задача 10. Допущена одна ошибка, позиция ошибки i = 13 ⇒ (1**0**01 0100 0011 101)

Критерии оценивания.

За выполнение каждого индивидуального задания выставляются оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если решение индивидуального задания полностью верное.

Оценка «хорошо» выставляется, если для решения индивидуального задания выбран верный алгоритм, но решение содержит арифметические ошибки, не оказавшие существенного влияния на результат.

Оценка «удовлетворительно» выставляется, если решение индивидуального задания содержит ошибки, существенно повлиявшие на результат.

Оценка «неудовлетворительно» выставляется, если решение индивидуального задания не доведено до конца или для его решения выбран неверный алгоритм.

Контрольные работы (ИОПК-3.2, ИОПК-3.3)

Контрольная работа 1

1. Неравенство Мак-Миллана. Может ли существовать двоичный код с длинами слов 1,2,2,3,3,3 ?

2. Алгоритм Шеннона: суть алгоритма. Используя алгоритм Шеннона, построить префиксный код для набора длин {2,3,3,3,4,4,4}.

Ответы:

Задача 1. Нет. Неравенство Мак-Миллана не выполнено.

Задача 2. C = {00, 010, 011, 100, 1010, 1011, 1100} .

Контрольная работа 2

1. Определение порождающего многочлена циклического кода. Какой многочлен может быть порождающим многочленом циклического кода? Докажите, что многочлен $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ можно использовать в качестве порождающего многочлена циклического (15,7)-кода. Определите, сколько ошибок будет исправлять этот код, если поле $GF(2^4)$ построено с помощью корня примитивного многочлена $x^4 + x + 1$.

2. Для рассмотренного в п. 2 кода, исправить ошибки в слове (1111 1000 1100 011).

Ответы:

Задача 1. Код исправляет 2 ошибки, т.к. a и a^3 являются корнями $g(x)$ (где a – примитивный элемент поля $GF(2^4)$.

Задача 2. Позиции ошибок: $x_1 = 2$, $x_2 = 12$ ⇒ (11**0**1 1000 1100 **1**11)

Критерии оценивания:

Результаты контрольной работы фиксируются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если даны правильные ответы на все теоретические вопросы и задачи решены без ошибок.

Оценка «хорошо» выставляется, если ответы на теоретические вопросы в целом правильные, но не полные. При решении задач выбраны верные алгоритмы и сделана правильная интерпретация результатов, но допущены ошибки арифметического характера.

Оценка «удовлетворительно» выставляется, если ответы на теоретические вопросы неполные и содержат незначительные ошибки. При решении задач выбраны верные алгоритм, но допущенные в ходе решения ошибки существенно повлияли на результат.

Оценка «неудовлетворительно» выставляется, если ответ студента на теоретические вопросы неполный и содержит серьезные ошибки. Решение задач не доведено до конца или выбран неверный алгоритм

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзаменационный билет состоит из двух частей.

Первая часть представляет собой два теоретических вопроса. Ответы на вопросы даются в развернутой форме и проверяют ИОПК-3.1.

Вторая часть представляет собой практическое задание и проверяет ИОПК-3.2 и ИОПК-3.3. Ответ предполагает выбор алгоритма для решения задачи, получение решения и интерпретацию полученного результата.

Продолжительность экзамена 1,5 часа.

а) Примерный перечень теоретических вопросов к экзамену.

1. Понятие кодирования и декодирования. Математическая постановка задачи кодирования и декодирования. Алфавитное кодирование.
2. Основные требования, предъявляемые к коду.
3. Когда кодирование называется однозначным. Необходимое и достаточное условие однозначного кодирования.
4. Три достаточных условия однозначности кода.
5. Критерий однозначности алфавитного кодирования Маркова. Его геометрическая формулировка. Уметь применять геометрический критерий на практике.
6. Оценка минимальной длины неоднозначно декодируемого слова.
7. Коэффициент избыточности кода (определение). Код с минимальной избыточностью (определение).
8. Неравенство Мак-Миллана. Может ли существовать двоичный код с длинами слов 1,2,2,3,3,3 ?
9. Когда неравенства Мак-Миллана приобретает достаточный характер.
10. Алгоритм Шеннона построения кода с заданными длинами слов.
11. Свойства оптимальных кодов
12. Алгоритм Фано. Алгоритм Хаффмана.
13. Типы ошибок, которые возникают при передаче информации.
14. Понятие блокового и древовидного кода. Основные определения, связанные с блоковым кодом (кодовые слова, длина кода, мощность кода)
15. Принцип максимального правдоподобия (суть), таблица кодирования (структура, принцип использования)
16. Метрическое пространство Хемминга. Вектор ошибок. Вес вектора ошибки и расстояние между принятым и переданным словом.
17. Кодовое расстояние. Связь кодового расстояния с возможностями кода исправлять и обнаруживать ошибки. Примеры.
18. Граница Хемминга.

19. Линейный код: определение, размерность линейного кода. Кодовое расстояние линейного кода. Мощность линейного кода.

20. Порождающая матрица линейного кода: определение, назначение. Проверочная матрица линейного кода: определение, назначение, определение кодового расстояния по проверочной матрице.

21. Исправление и обнаружение ошибок линейными кодами: стандартное расположение для таблицы декодирования, необходимое и достаточное условие исправления ошибки в случае стандартного расположения для таблицы декодирования.

22. Понятие синдрома вектора. Алгоритм декодирования с использованием синдрома.

23. Верхняя граница линейного кода (граница Плоткина). Может ли существовать линейный (7,4)-код, исправляющий 2 ошибки?

24. Граница Синглтона. Граница Варшамова-Гильберта.

25. Код Хемминга: с длиной кодового слова $n = 2^m - 1$, с произвольной длиной слова. Кодовое расстояние для кода Хемминга. Декодирование кода Хемминга. Кодирование кодом Хемминга.

26. Коды Рида-Маллера: построение порождающей матрицы кода Рида-Маллера r-го порядка длины 2^m, кодовое расстояние.

27. Декодирование кодов Рида-Маллера: мажоритарный принцип декодирования, порядок декодирования информационных символов, принцип построения проверочных сумм для информационных символов 1-го, 2-го и т.д. порядков.

28. Циклический код: определение, соответствие кодовое слово – многочлен, связь циклического сдвига вектора с умножением классов вычетов многочленов.

29. Описание циклических кодов с помощью многочленов: умножение (по модулю $x^n - 1$) слова циклического кода на произвольный многочлен, определение порождающего многочлена, степень порождающего многочлена, деление кодовых слов на порождающий многочлен, теорема о том, какие многочлены могут быть порождающими многочленами циклических кодов.

30. Порождающая и проверочная матрица циклического кода. Описание циклического кода посредством корней порождающего многочлена. Проверочная матрица кода в поле $GF(2^m)$ – расширении поля GF(2).

31. Исправление ошибок циклическими кодами. Теорема Меггита. Алгоритм исправления ошибок, использующий теорему Меггита. Исправление пактов ошибок циклическими кодами.

32. Циклический код, исправляющий две ошибки. Теорема о границе БЧХ. БЧХ-коды. Построение порождающего многочлена БЧХ-кода.

33. Общий случай декодирования двоичных кодов БЧХ.

34. Древовидный код: отличие от блокового кода, кодирование и декодирование древовидных кодов (общий принцип). Связь кодового расстояния с возможностями древовидного кода исправлять и обнаруживать ошибки.

35. Линейный древовидный код: определение, порождающая матрица. Сверточные коды. Сверточные (n,k)-коды. Связь кодового расстояния сверточного кода с проверочной матрицей.

36. Алгоритм Витерби (суть)

б) Примеры задач.

В экзаменационный билет включаются задачи того же типа, чти и в индивидуальное задание и контрольные работы.

в) Критерии оценивания.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если:
а) студент дал полный и развернутый ответ на теоретические вопросы;
б) решение практического задания верное.

Оценка «хорошо» выставляется, если:
а) ответ студента на теоретические вопросы в целом полный, но имеются незначительные замечания;
б) решение практического задания верное или содержит арифметические ошибки, не влияющие на используемый алгоритм

Оценка «удовлетворительно» выставляется, если:
а) ответ студента на теоретические вопросы не полный;
б) решение практического задания содержит ошибки, существенно повлиявшие на результат.

Оценка «неудовлетворительно» выставляется, если:
а) ответ студента на теоретические вопросы не полный и содержит серьезные ошибки;
б) решение практического задания не доведено до конца или для его решения выбран неверный алгоритм.

Если в течение семестра студент посетил не менее 75% занятий и выполнил все контрольные работы и индивидуальное задание на положительную оценку, то он освобождается от выполнения практической части билета.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы

1. Понятие кодирования и декодирования. Математическая постановка задачи кодирования и декодирования. Алфавитное кодирование.
2. Основные требования, предъявляемые к коду.
3. Коэффициент избыточности кода (определение). Код с минимальной избыточностью (определение).
4. Понятие блокового и древовидного кода. Основные определения, связанные с блоковым кодом (кодовые слова, длина кода, мощность кода)
5. Принцип максимального правдоподобия (суть), таблица кодирования (структура, принцип использования)
6. Вектор ошибок. Вес вектора ошибки и расстояние между принятым и переданным словом.
7. Кодовое расстояние. Связь кодового расстояния с возможностями кода исправлять и обнаруживать ошибки.
8. Линейный код: определение, размерность линейного кода. Кодовое расстояние линейного кода. Мощность линейного кода.
9. Порождающая матрица линейного кода: определение, назначение. Проверочная матрица линейного кода: определение, назначение, определение кодового расстояния по проверочной матрице.
10. Исправление и обнаружение ошибок линейными кодами: стандартное расположение для таблицы декодирования, необходимое и достаточное условие исправления ошибки в случае стандартного расположения для таблицы декодирования.
11. Понятие синдрома вектора. Алгоритм декодирования с использованием синдрома.
12. Древовидный код: отличие от блокового кода, кодирование и декодирование древовидных кодов (общий принцип). Связь кодового расстояния с возможностями древовидного кода исправлять и обнаруживать ошибки.

Задачи

Задача 1 (ИОПК-3.2, ИОПК-3.3)

Найдите кодовое слово, в которое линейный (5,3)-код с порождающей матрицей $\mathbf{G}=\begin{pmatrix}1&0&0&1&0\\0&1&0&0&1\\0&0&1&1&1\end{pmatrix}$ кодирует информационное слово u=(011).

Задача 2 (ИОПК-3.2, ИОПК-3.3)

Найдите проверочную матрицу для линейного (5,3)-кода с порождающей матрицей $\mathbf{G}=\begin{pmatrix}1&0&0&1&0\\0&1&0&0&1\\0&0&1&1&1\end{pmatrix}$. Проверить, являются ли кодовыми слова (101000) и (11111). Используя синдром, исправить ошибку в слове, не являющимся кодовым.

Ответы к задачам:

Задача 1. (01111) .

Задача 2. $\mathbf{H}=\begin{pmatrix}1&0&1&1&0\\0&1&0&0&1\end{pmatrix}$, (101000) – кодовое слово, (11111) – не кодовое слово; синдром – (10) .

Информация о разработчиках

Пахомова Елена Григорьевна, канд. физ.-мат. наук, доцент, кафедра компьютерной безопасности, доцент.