Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теория информации

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов 4 курса очной формы обучения

Уровень высшего образования
СПЕЦИАЛИТЕТ

Составитель:

д.ф.-м.н., профессор Г.С. Шаров

Тверь 2023

I. Аннотация

1. Наименование дисциплины в соответствии с учебным планом

Теория информации

2. Цель и задачи дисциплины

Целями освоения дисциплины «Теория информации» являются:

1. фундаментальная подготовка в области теории информации и теории кодирования;
2. овладение современным математическим аппаратом для дальнейшего использования в приложениях.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока дисциплин, формирующих общепрофессиональные компетенции. Для ее успешного освоения необходимы знания и умения, приобретенные в результате обучения дисциплинам: алгебра, математический анализ, теория вероятностей и математическая статистика и др.

4. Объём дисциплины:

3 зачетных единицы, 108 академических часов, в том числе
контактная работа: лекции – 36 часов, практические занятия – 36 часов, самостоятельная работа – 36 часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине**
ОПК-3 способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** основами построения моделей текстовой информации и моделей систем передачи информации **Уметь** вычислять теоретико-информационные характеристики информационных сообщений и каналов связи (энтропии, взаимная информация, пропускная способность). **Знать:** основные понятия и методы теории информации: понятия энтропии, информационной дивергенция, взаимной информации, дискретного источника без памяти, канала связи, основные методы теории коди-

	рования

6. Форма промежуточного контроля

Зачёт.

7. Язык преподавания

русский.

II. Структура дисциплины (модуля)

1. Структура дисциплины (модуля) для студентов очной формы обучения

Наименование разделов и тем	Всего	Аудиторные занятия		Самостоят. работа
		Лекции	Практические	
1. Энтропия случайной величины (дискретного источника), ее свойства. Аксиомы Хинчина и Фаддеева. Дискретный источник без памяти, двоичный (k,n)-блоковый код, его ошибка, теорема Шеннона.	12	4	4	4
2. Информационная дивергенция двух распределений случайных величин, ее неотрицательность. Условная энтропия случайных величин, условная энтропия для независимых случайных величин. Взаимная информация случайных величин, ее свойства и выражение через информационную дивергенцию. Марковские источники.	16	6	6	4
3. Коды с постоянной длиной на входе и/или выходе ((k,n)-блоковые коды). Коды с переменной длиной на выходе. Разделимые коды, свойство префикса, префиксные коды, кодовое дерево. Неравенство Крафта для префиксного кода.	8	3	3	2
4. Линейный (k,n)-блоковый код. Конечные поля $GF(q)$. Порождающая матрица. Помехоустойчивый линейный (k,n)-блоковый код. Поля Галуа. Порождающая матрица. Проверочные уравнения и проверочная матрица. Расстояние Хэмминга, кодовое расстояние кода, его связь с числом проверочных символов и линейно зависимыми строками проверочной матрицы. Стандартное распределение для линейного кода. Принцип построения кода Хэмминга, его кодовое расстояние. Проверочные уравнения для кода Хэмминга.	24	8	8	8
5. Циклический линейный (k,n)-блоковый код. Порождающий и проверочный многочлены циклического кода, их порядок связь с порождающей и проверочной матрицами; кодовое расстояние циклического кода.	16	5	6	5

6. Принцип построения БХЧ-кода. Порождающий и проверочный многочлены, их порядок, ограниченность значений порождающего многочлена значениями в GF(2). Коды Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние	12	4	4	4
7. Математическая модель канала связи, стохастическая матрица, дискретный канал без памяти. Пропускная способность канала связи. Прямая и обратная теорема кодирования.	20	8	6	6
Итого	108	36	36	36

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Учебная программа

1. Энтропия случайной величины (дискретного источника), ее свойства; аксиомы Хинчина.
2. Дискретный источник без памяти, двоичный (k,n)-блоковый код, его ошибка, теорема Шеннона.
3. Информационная дивергенция двух распределений случайных величин, ее неотрицательность.
4. Условная энтропия случайных величин, условная энтропия для независимых случайных величин. Взаимная информация случайных величин, ее свойства и выражение через информационную дивергенцию.
5. Коды с постоянной длиной на входе и/или выходе ((k,n)-блоковые коды). Коды с переменной длиной на выходе. Разделимые коды, свойство префикса, префиксные коды, кодовое дерево. Неравенство Крафта для префиксного кода.
6. Линейный (k,n)-блоковый код, помехоустойчивый линейный (k,n)-блоковый код. Конечные поля. Порождающая матрица. Проверочные уравнения и проверочная матрица.
7. Расстояние Хэмминга, кодовое расстояние кода, его связь с числом проверочных символов и линейно зависимыми строками проверочной матрицы линейного (k,n)-блокового кода. Исправление одиночных ошибок.
8. Принцип построения кода Хэмминга, его кодовое расстояние. Проверочные уравнения для кода Хэмминга.
9. Циклический линейный (k,n)-блоковый код. Порождающий и проверочный многочлены циклического кода, их порядок связь с порождающей и проверочной матрицами; кодовое расстояние циклического кода.
10. Принцип построения БХЧ-кода. Порождающий и проверочный многочлены, их порядок, ограниченность значений порождающего многочлена значениями в GF(2).
11. Коды Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние.
12. Математическая модель канала связи, стохастическая матрица, дискретный канал без памяти. Пропускная способность канала связи. Прямая и обратная теорема кодирования.

Вариант 1

1. Дайте определение энтропии случайной величины (энтропии дискретного источника). В каком случае эта величина достигает минимума. Обоснуйте.

2. Даны случайные величины X, X^2, X^3. Какая из взаимных информаций $I(X,X^2)$, $I(X,X^3)$, $I(X^3,X^2)$ максимальна и минимальна?

3. Докажите неравенство Крафта для префиксного кода.

Вариант 2

1. Дайте определение информационной дивергенции двух случайных величин, доказательство ее неотрицательности.

2. Сравните энтропии двух случайных величин X и $f(X)$.
3. Является ли $GF(4)$ (кольцо вычетов по модулю 4) полем, почему? Дайте определение линейного кода, постройте пример кода с алфавитом $GF(4)$.

Вариант 4

1. Дайте определение условной энтропии и взаимной информации случайных величин, условная энтропия для независимых случайных величин.
2. Сравните взаимные информации случайных величин $I(X,Y)$ и $I(f(X),Y)$.
3.Помехоустойчивый линейный (k,n)-блоковый код. Кодовое расстояние (Хэмминга) кода, его связь со строками проверочной матрицы.

Контрольная работа № 2

Вариант 1

1. Помехоустойчивый линейный (k,n)-блоковый код. Кодовое расстояние (Хэмминга) кода, его связь со строками проверочной матрицы.
2. Постройте пример линейного циклического кода с $k = 2$, $n = 4$, с троичным алфавитом $GF(3)$. Найдите кодовое расстояние d_0.

Вариант 2

1. Принцип построения циклического линейного (k,n)-блокового кода. Порождающий и проверочный многочлены, их порядок, соответствующие матрицы.
2. Постройте пример линейного (не циклического) (k,n)-блокового кода с алфавитом $GF(5)$ с кодовым расстоянием $d_0 \geq 3$.

Вариант 3

1. Дайте определение линейного (k,n)-блокового кода, порождающей матрицы, ее связь с проверочной матрицей.
2. Постройте пример циклического линейного кода с $n = 6$ и порождающим многочленом $g = t^2+t+1$ (q выберите сами). Найдите порождающую, проверочную матрицы, кодовое расстояние d_0.

Вариант 4

1. Принцип построения кода Хэмминга, его кодовое расстояние d_0. Привести пример кода Хэмминга для с $n = 15$ с порождающей и проверочной матрицами, найти d_0, составить проверочные уравнения.
2. Число различных невырожденных квадратных матриц над полем $GF(q)$.

Контрольная работа № 3

Вариант 1

1. Описав принципы построения, приведите пример линейного (не циклического) (k,n)-блокового кода с алфавитом $GF(2)$ с кодовым расстоянием $d_0=3$.
2. Найдите количество различных невырожденных квадратных матриц над полем $GF(q)$.
3. Постройте поле $GF^*(3^2)$ – расширение $GF(3)$ по модулю
$P_2 = 2z^2 + z + a_0$ (обосновав выбор a_0). С его помощью постройте код БХЧ, исправляющий $N_u = 1$ ошибку. Найдите значения k, n, r, порождающий и проверочный многочлены, соответствующие матрицы, кодовое расстояние d_0. Приведите пример исправления 1 ошибки в кодовом слове и последующего декодирования.

Вариант 2

1. Помехоустойчивый линейный (k,n)-блоковый код. Кодовое расстояние кода, его связь со строками проверочной матрицы.

2. Постройте пример линейного циклического кода с $k = 2$, $n = 4$, с троичным алфавитом $GF(3)$. Найдите кодовое расстояние d_0.
3. Постройте поле $GF^*(2^3)$ – расширение $GF(2)$ по модулю
$P_3 = z^3 + z^2 + 1$. С его помощью постройте код Рида-Соломона с $r = 2$. Найдите значения k, n, порождающий и проверочный многочлены, соответствующие матрицы (можно схематично), кодовое расстояние d_0. Приведите пример исправления 1 ошибки в кодовом слове и последующего декодирования.

Вопросы к зачету

1. Дайте определение энтропии случайной величины (энтропии дискретного источника). В каком случае эта величина достигает минимума?
2. Даны случайные величины X, X^2, X^3. Какая из взаимных информаций $I(X,X^2)$, $I(X,X^3)$, $I(X^3,X^2)$ максимальна и минимальна?
3. Дайте определение информационной дивергенции двух случайных величин, доказательство ее неотрицательности.
5. Сравните энтропии двух случайных величин X и $f(X)$.
6. Дайте определение дискретного источника без памяти, двоичного (k,n)-блокового кода, его ошибки и формулировка теоремы Шеннона.
7. Определение условной энтропии и взаимной информации случайных величин, условная энтропия для независимых случайных величин.
8. Сравните взаимные информации случайных величин $I(X,Y)$ и $I(f(X),Y)$.
9. Выражение взаимной информации двух случайных величин через информационную дивергенцию (с доказательством).
10. Докажите неотрицательность взаимной информации двух случайных величин.
11. Дайте определение префиксного кода, постройте пример кодового дерева с троичным алфавитом кода.
12. Докажите неравенство Крафта для префиксного кода.
13. Принцип построения помехоустойчивого линейного (k,n)-блокового кода. Порождающая матрица. Проверочные уравнения и проверочная матрица. Стандартное распределение. Пример кода Хэмминга.
14. Принцип построения помехоустойчивого линейного (k,n)-блокового кода. Кодовое расстояние (Хэмминга) кода, его связь со строками проверочной матрицы. Пример кода Рида-Соломона.
15. Принцип построения кода Хэмминга, его кодовое расстояние. Привести пример кода Хэмминга с порождающей и проверочной матрицами, составить проверочные уравнения.
16. Принцип построения циклического линейного (k,n)-блокового кода. Порождающий и проверочный многочлены, их порядок; кодовое расстояние. Привести пример циклического кода.
17. Принцип построения БХЧ-кода. Порождающий и проверочный многочлены, их порядок. Привести пример такого кода.
18. Принцип построения кода Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние. Привести пример такого кода.
19. Канал связи, стохастическая матрица, дискретный канал без памяти, пропускная способность канала связи.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

1. Типовые контрольные задания для проверки уровня сформированности компетенции.

Этап формирования	Типовые контрольные	Показатели и крите-

компетенции, в котором участвует дисциплина	задания для оценки знаний, умений, навыков (2-3 примера)	рии оценивания компетенции, шкала оценивания
владеть	Принцип построения кода Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние. Привести пример такого кода.	Уверенное владение, задание полностью выполнено – 7 баллов. Наличие отдельных ошибок – 3 – 6 баллов. Большое количество ошибок – 0 баллов.
уметь	Выражение взаимной информации двух случайных величин через информационную дивергенцию (с доказательством).	Правильное выполнение задания – 6 баллов. Наличие отдельных ошибок – 3 – 5 баллов. Большое количество ошибок, решение не дано или дано неверное решение– 0 баллов.
знать	Дайте определение энтропии случайной величины (энтропии дискретного источника). В каком случае эта величина достигает минимума и максимума?	Глубокие знания – 6 баллов. Неуверенные знания – 3 – 5 баллов. Серьезные пробелы в знаниях, ошибки – 0 баллов

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Основная литература:

Чуканов С. Н. Теория информации [Электронный ресурс] : учебное пособие / С. Н. Чуканов. - Омск : ОмГТУ, 2022. - 192 с. - Книга из коллекции ОмГТУ - Информатика. Режим доступа: https://e.lanbook.com/book/343790
Попов, И. Ю. Теория информации : учебник для вузов / И. Ю. Попов, И. В. Блинова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 160 с. — ISBN 978-5-8114-8338-9. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175153

б) дополнительная литература:

Котенко В.В. Теория информации и защита телекоммуникаций [Электронный ресурс] : монография / В.В. Котенко, К.Е. Румянцев. — Электрон. текстовые данные. — Ростов-на-Дону: Южный федеральный университет, 2009. — 372 с. — 978-5-9275-0670-5. — Режим доступа: http://www.iprbookshop.ru/47155.html

Балюкевич Э.Л. Теория информации : учебное пособие / Балюкевич Э.Л.. — Москва : Евразийский открытый институт, 2009. — 215 c. — ISBN 978-5-374-00219-5. — Текст : электронный // ЭБС IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10863.html
Лидовский, В.В. Основы теории информации и криптографии : курс / В.В. Лидовский ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2007. - 125 с. : табл., схем. ; То же [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=234148

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

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.

VII. Методические указания для обучающихся по освоению дисциплины

Для успешного усвоения материала данной учебной дисциплины, в частности, для выработки навыков решения задач необходима систематическая самостоятельная работа студентов по подготовке к практическим занятиям, коллоквиумам и к контрольным работам.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (по необходимости)

1. Лекция с использованием средств мультимедиа.
2. Практическое занятие с использованием средств мультимедиа.

Программное обеспечение:

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски.

X. Сведения об обновлении рабочей программы дисциплины

№ п.п.	Обновленный раздел рабочей программы дисциплины (модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1	Разделы: компетенции, литература	Приведение в соответствие новым требованиям	09.06.2015 г, протокол № 7
2			