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

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теория информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов 3 курса очной формы обучения

Составитель:
д. ф.-м. н., профессор Шаров Г.С.

Тверь 2023

I. Аннотация

1. 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.

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть учебного плана. Для ее успешного освоения необходимы знания и умения, приобретенные в результате обучения дисциплинам: алгебра, математический анализ, теория вероятностей и математическая статистика и др.

3. Объём дисциплины:

4 зачетных единицы, 144 академических часа, в том числе
контактная работа: лекции – 34 часа, в т.ч. практическая подготовка 0 часов, практические занятия – 34 часов; самостоятельная работа – 76 часов.

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 при-

	кладных 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

5. Форма промежуточного контроля

Зачёт.

6. Язык преподавания

русский.

II. Структура дисциплины (модуля)

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

Наименование разделов и тем	Всего	Контактная работа (час.)			Самостоят. работа
		Лекции	Практические	Практич. подготовка	
1. Энтропия случайной величины (дискретного источника), ее свойства. Дискретный источник без памяти, двоичный (k,n)-блоковый код, его ошибка, теорема Шеннона.	18	4	4	0	10
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.	26	6	6	0	14
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.	12	3	2	0	7

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 с проверочной матрицей. Принцип построения кода Хэмминга, его кодовое расстояние, проверочные уравнения.	30	6	7	0	15
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.	21	5	6	0	10
6. Коды Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние. Принцип построения БХЧ-кода. Порождающий и проверочный многочлены, их порядок, алфавит.	16	4	4	0	8
7. Математическая модель канала связи, стохастическая матрица, дискретный канал без памяти. Пропускная способность канала связи. Прямая и обратная теорема кодирования.	24	6	5	0	12
Итого	144	34	34	0	76

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Тема 1. Энтропия случайной величины	лекция практическое	Классическая лекция, дискуссионные технологии, , технология развития креативного мышления
Тема 2. Информационная дивергенция, условная энтропия, взаимная информация.	лекция практическое	Классическая лекция, проблемная лекция, дискуссионные технологии, методы группового решения творческих задач.
Тема 3. Коды с переменной длиной на выходе, префиксные коды,	лекция практическое	Проблемная лекция, игровая технология, кейс-технология, методы группового решения творческих задач.
Тема 4. Линейный (k,n)-блоковый помехоустойчивый код	лекция практическое	Классическая лекция, мозговой штурм, дискуссионные технологии, методы группового решения творческих задач.

Тема 5. Циклический линейный (k,n)-блоковый код.	лекция практическое	Проблемная лекция, мозговой штурм, методы группового решения творческих задач.
Тема 6. Коды Рида-Соломона, БХЧ-коды	лекция практическое	Классическая лекция, методы группового решения творческих задач.
Тема 7. Математическая модель канала связи, теоремы кодирования.	лекция практическое	Классическая лекция, мозговой штурм, дискуссионные технологии, технология развития креативного мышления.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

Проверяемые компетенции: ОПК–3, ОПК–8.

Контрольная работа № 1

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.

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.

Оценочные материалы для проведения промежуточной аттестации

Проверяемые компетенции: ОПК–3, ОПК–8, ОПК–10.

Примеры заданий:

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

Критерии оценивания и шкала оценивания:

Глубокие знания – 6 баллов, неуверенные знания – 3 – 5 баллов.
Серьезные пробелы в знаниях, ошибки – 0 баллов

2. Выражение взаимной информации двух случайных величин через информационную дивергенцию (с доказательством).

Критерии оценивания и шкала оценивания:

Правильное выполнение задания – 6 баллов. Наличие отдельных ошибок – 3 – 5 баллов. Большое количество ошибок, решение не дано или дано неверное решение– 0 баллов.

3. Принцип построения кода Рида-Соломона. Порождающий и проверочный многочлены, их порядок и кодовое расстояние. Привести пример такого кода.

Критерии оценивания и шкала оценивания:

Задание полностью выполнено – 7 баллов. Наличие отдельных ошибок – 3 – 6 баллов. Большое количество ошибок – 0 баллов.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература:

1. 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
2. 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:

1. 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 c. — 978-5-9275-0670-5. — Режим доступа: http://www.iprbookshop.ru/47155.html
2. 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
3. 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

2) 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

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.

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

http://www.exponenta.ru сайт с математическими продуктами и приложениями

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

VI. Методические материалы 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 и к контрольным работам.

Планы практических (семинарских) занятий и методические рекомендации к ним.

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.

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.

Требования к рейтинг-контролю для студентов

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом 1 модуль – 35 баллов, 2 модуль – 65 баллов.

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 помещений**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
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 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Мультимедийный комплект учебного класса (вариант № 2): Проектор Casio XJ-140 настенный проекц. экран Lumien 180*180, Ноутбук Dell N4050, сумка 15,6", мышь; Усилитель Roxton AA-120; Радиосистема Shure PG288/PG58; Микшер Mackie 402 VLZ; Стационарный микрофон SOUNDKING EG002 с настольным держателем; Мультимедийный проектор Casio XJ-H2650 с потолоч. крепл. и мотириз. экраном	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
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 № 224 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Набор учебной мебели, меловая доска, Переносной ноутбук, Мультимедийный проектор BenQ MP 724 с потолочным креплением и экраном 1105	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
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индиви-	Набор учебной мебели, меловая доска, Переносной ноутбук, Интерактивная система Smart Board 660iv со встроенным проектором	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus – бесплатно; OpenOffice –

дуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 207 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)		бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно

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.	Разделы I - VII.	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
2.	I. Компетенции. V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Изменение компетенций и индикаторов. Дополнение списков литературы. Обновление ссылок из ЭБС.	Протокол № 3 от 26.11.2020
3.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
4.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023