Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
и.о. заведующего кафедрой
Борисов Дмитрий Николаевич
Кафедра информационных систем
21.04.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.28 Теория информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Анализ безопасности компьютерных систем, Математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалитет

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра информационных систем

6. Составители программы:

Борисов Дмитрий Николаевич (borisov@cs.vsu.ru)

7. Рекомендована:

протокол НМС №5 от 10.03.2021

8. Учебный год:

2023-2024

9.Цели и задачи учебной дисциплины:

Цель изучения дисциплины – формирование у обучающихся фундаментальных теоретических знаний в области дискретных источников сообщений, неравномерного кодирования дискретных источников; кодирования дискретных источников при неизвестной статистике; алгоритмов кодирования источников, применяемые в архиваторах; кодирования для дискретных каналов с шумом. В результате изучения дисциплины обучающиеся должны освоить теоретические основы кодирования информации, изучить основные алгоритмы построения эффективных кодов, используемых, в том числе и для сжатия информации. Кроме того обучающиеся должны освоить методику решения различных задач, связанных с процессами получения, передачи, хранения и использования информации.

Задачи изучения дисциплины:

- формирование у обучающихся систематических знаний в области теоретического кодирования информации;
- ознакомление обучающихся с перспективными направлениями в области сжатия информации;

- обучение обучающихся вопросам построения эффективных кодов, используемых для передачи информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к обязательной части блока Б1. Для изучения дисциплины необходимо знать алгебру, Алгоритмы и структуры данных, теория вероятностей и математическая статистика (4 семестр)

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.21 знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации;	**знать:** фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.22 знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума;	**знать:** основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.23 знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга);	**знать:** основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга)
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.24 знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования;	**знать:** понятие пропускной способности канала связи, прямую и обратную теоремы кодирования
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.25 умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность);	**уметь:** вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.26 умеет решать типовые задачи кодирования и декодирования;	**уметь:** решать типовые задачи кодирования и декодирования
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.27 владеет основами построения математических моделей текстовой информации и моделей систем передачи информации;	**владеть:** основами построения математических моделей текстовой информации и моделей систем передачи информации;
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.28 владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.	**владеть:** навыками применения математического аппарата для решения прикладных теоретико-информационных задач

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 5	Всего
Аудиторные занятия	50	50
Лекционные занятия	34	34
Практические занятия		0
Лабораторные занятия	16	16
Самостоятельная работа	22	22
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.1	Энтропия дискретных источников	Дискретные источники сообщений. Измерение информации. Собственная информация. Энтропия. Выпуклые функции многих переменных. Условная энтропия. Дискретные случайные последовательности. Цепи Маркова. Энтропия на сообщение дискретного стационарного источника. Равномерное кодирование дискретного источника. Постановка задачи. Неравенство Чебышева. Закон больших чисел. Прямая теорема кодирования для дискретного постоянного источника. Обратная теорема кодирования для дискретного постоянного источника. Множество типичных последовательностей для дискретного постоянного источника. Источники с памятью.	https://edu.vsu.ru/course/view.php?id=6563#section-5

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.2	Неравномерное кодирование дискретных источников	Постановка задачи неравномерного побуквенного кодирования. Неравенство Крафта. Теоремы побуквенного неравномерного кодирования. Оптимальный побуквенный код – код Хаффмана. Избыточность кода Хаффмана. Код Шеннона. Код Гилберта-Мура. Неравномерное кодирование для стационарного источника.	https://edu.vsu.ru/course/view.php?id=6563#section-6
1.3	Кодирование дискретных источников при неизвестной статистике	Постановка задачи универсального кодирования источников. Несколько полезных комбинаторных формул. Двухпроходное побуквенное кодирование. Нумерационное кодирование. Асимптотические границы избыточности универсального кодирования. Адаптивное кодирование. Сравнение алгоритмов.	https://edu.vsu.ru/course/view.php?id=6563#section-7

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.4.	Алгоритмы кодирования источников, применяемые в архиваторах	Монотонные коды. Интервальное кодирование и метод «стопка книг». Метод скользящего словаря (LZ-77). Алгоритм LZW (LZ-78). Предсказание по частичному совпадению. Сжатие с использованием преобразования Барроуза-Уилера. Сравнение способов кодирования. Характеристики архиваторов.	https://edu.vsu.ru/course/view.php?id=6563#section-8

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.5	Кодирование для дискретных каналов с шумом	Постановка задачи помехоустойчивого кодирования. Модели каналов. Взаимная информация. Средняя взаимная информация. Условная средняя взаимная информация. Теорема о переработке информации. Выпуклость средней взаимной информации. Информационная емкость и пропускная способность. Неравенство Фано. Обратная теорема кодирования. Вычисление информационной емкости каналов без памяти. Симметричные каналы. Прямая теорема кодирования для дискретных постоянных каналов. Типичные пары последовательностей. Типичные пары последовательностей.	https://edu.vsu.ru/course/view.php?id=6563#section-9
2. Лабораторные работы			
2.1	Ансамбли и вероятности	Вероятностные ансамбли. Байесовский вывод.	https://edu.vsu.ru/course/view.php?id=6563#section-15
2.2	Энтропия	Энтропия. Условная энтропия и ее свойства. Энтропия дискретного источника информации. Полная и частная энтропии.	https://edu.vsu.ru/course/view.php?id=6563#section-15

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2.3	Марковские цепи	Стационарные Марковские цепи. Расчет условной энтропии стационарной Марковской цепи.	https://edu.vsu.ru/course/view.php?id=6563#section-16
2.4	Количество информации	Расчет количества информации. Свойства количества информации.	-
2.5	Неравномерное кодирование	Код Хаффмана. Код Шеннона-Фано. Код Гилберта-Мура. Арифметическое кодирование.	https://edu.vsu.ru/course/view.php?id=6563#section-18
2.6	Блоковый источник с n-кратным расширением	Кодирование блокового источника X2 и X3.	https://edu.vsu.ru/course/view.php?id=6563#section-18
2.7	Универсальный алгоритм сжатия	Алгоритм универсального кодирования Лемпеля-Зива. Декодирование LZ-кода. Алгоритм Лемпеля-Зива-Уэлча. Декодирования LZW.	https://edu.vsu.ru/course/view.php?id=6563#section-19
2.8	Каналы без памяти	Двоичный симметричный канал без памяти. Комбинирование источников.	-
2.9	Пропускная способность канала	Средняя взаимная информация. Пропускная способность двоичного симметричного канала.	-

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Энтропия дискретных источников	6		3	4	13
2	Неравномерное кодирование дискретных источников	7		3	5	15
3	Кодирование дискретных источников при неизвестной статистике	7		3	5	15
4	Алгоритмы кодирования источников, применяемые в архиваторах	7		4	4	15
5	Кодирование для дискретных каналов с шумом	7		3	4	14
		34	0	16	22	72

14. Методические указания для обучающихся по освоению дисциплины

Для успешного освоения дисциплины рекомендуется систематическая подготовка к выполнению практических заданий, а также самостоятельная работа обучающегося, которая предусматривает подготовку к рубежным аттестациям и изучение дополнительной литературы по вопросам дисциплины.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Трухан, А. А. Теория вероятностей в инженерных приложениях : учебное пособие / А. А. Трухан, Г. С. Кудряшев. — 4-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2015. — 368 с. — ISBN 978-5-8114-1664-6. — Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/reader/book/56613/#1

б) дополнительная литература:

№ п/п	Источник
1	Котенко В. В. Теория информации: учебное пособие / В. В. Котенко, К.Е. Румянцев. - Ростовна-Дону, Таганрог: Ихздательство Южного федерального университета, 2018. - 240 с. Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=561095
2	Осокин, А. Н. Теория информации : учебное пособие / А. Н. Осокин, А. Н. Мальчуков. — Томск : ТПУ, 2014. - 2006 с. - Лань : электронно-библиотечная система. — Режим доступа : hhttps://e.lanbook.com/reader/book/62935/#1
3	Майстренко Н. В. Основы теории информации и криптографии : учебное электронное издание: учебное пособие / Н. В. Майстренко , А. В. Майстренко. - Тамбов: Издательский центр ФГБОУ ВО ТГТУ, 2018. - 81 с. - Университетская библиотека онлайн : электроннобиблиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=570354
4	Усенко О. А. Приложения теории информации и криптографии в радиотехнических системах: учебное пособие / О. А. Усенко. - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2017. - 239 с. - Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=500141
5	Волынская А.В. Теория информации: практикум / А.В. Волынская , Г.А. Черезов. - Издательство Уральского государственного университета путей сообщения, 2018. - 32 с. Лань: электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/reader/book/121385/#1

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	www.lib.vsu.ru ЗНБ ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	ЭУМК. Электронный университет ВГУ. - Режим доступа : https://edu.vsu.ru/course/view.php?id=6563

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Пакет математического программирования Matlab любой версии

18. Материально-техническое обеспечение дисциплины:

лекционная аудитория, оснащенная мультимедиа проектором; класс для проведения практических занятий; вычислительные устройства для проведения расчетов алгебраических функций до третьегознака после десятичного разделителя.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Энтропия дискретных источников	ОПК-10	ОПК-10.21	контрольное задание 1 тестовое задание 1
2	Неравномерное кодирование дискретных источников Кодирование дискретных источников при неизвестной статистике	ОПК-10	ОПК-10.22	контрольное задание 2 тестовое задание 2
3	Кодирование дискретных источников при неизвестной статистике Алгоритмы кодирования источников, применяемые в архиваторах Кодирование для дискретных каналов с шумом	ОПК-10	ОПК-10.23	контрольное задание 2 тестовое задание 2 контрольное задание 4
4	Кодирование дискретных источников при неизвестной статистике Алгоритмы кодирования источников, применяемые в архиваторах	ОПК-10	ОПК-10.24	контрольное задание 2 тестовое задание 2 контрольное задание 3 тестовое задание 3
5	Кодирование дискретных источников при неизвестной статистике Алгоритмы кодирования источников, применяемые в архиваторах Кодирование для дискретных каналов с шумом	ОПК-10	ОПК-10.25	контрольное задание 4

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
6	Кодирование дискретных источников при неизвестной статистике Алгоритмы кодирования источников, применяемые в архиваторах	ОПК-10	ОПК-10.26	контрольное задание 2 тестовое задание 2 контрольное задание 3 тестовое задание 3
7	Алгоритмы кодирования источников, применяемые в архиваторах	ОПК-10	ОПК-10.27	контрольное задание 3 тестовое задание 3
8	Кодирование дискретных источников при неизвестной статистике Алгоритмы кодирования источников, применяемые в архиваторах Кодирование для дискретных каналов с шумом	ОПК-10	ОПК-10.28	контрольное задание 2 тестовое задание 2 контрольное задание 4

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Для оценивания результатов обучения на экзамене используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Сформированные знания о фундаментальных положениях теории информации в части кодирования информации, передачи информации от различных источников по каналам. Сформированное умение формализовать задачу оценки информационных характеристик системы передачи информации, провести анализ ее работы и выделить наиболее значимые параметры Сформированы навыки анализа информационных характеристик системы передачи информации	*Повышенный уровень*	*Отлично*

Сформированные, но содержащие отдельные пробелы представления о фундаментальных положениях теории информации в части кодирования дискретных источников информации, алгоритмов кодирования источников. Успешное, но содержащее отдельные пробелы, умение формализовать задачу оценки информационных характеристик системы передачи информации, провести анализ ее работы и выделить наиболее значимые параметры Сформированы, но имеют отдельные пробелы, навыки анализа информационных характеристик системы передачи информации	*Базовый уровень*	*Хорошо*
Неполное представление о фундаментальных положениях теории информации в части кодирования дискретных источников при неизвестной статистике Умение формализовать задачу оценки информационных характеристик системы передачи информации, провести анализ ее работы и выделить наиболее значимые параметры, сопряженное с наличием существенных ошибок и способностью исправления при указании на них Сформированы, но имеют существенные пробелы, навыки анализа информационных характеристик системы передачи информации	*Пороговый уровень*	*Удовлетвори-тельно*
Фрагментарные знания или отсутствие знаний Фрагментарные умения или отсутствие умений Отсутствие навыков	–	*Неудовлетвори-тельно*

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью контрольных рапбот и тестовых заданий.

Контрольные (практико-ориентированные) задания Пример контрольного задания 1.

Дано произведение ансамблей XY=[x1y1 x1y2 x1y3 x2y1 x2y2 x2y3]

[0.21 0.42 0.07 0.09 0.18 0.03]

Определить, являются ли ансамбли X и Y независимыми, вычислить энтропию H(X), H(Y), H(XY).

Пример контрольного задания 2.

Для набора вероятностей построить код Хаффмана, Шеннона, Гильберта-Мура, арифметического кодирования.

z1 =0.249, z2 =0.03, z3 =0.085, z4 =0.04, z5 =0.11, z6 =0.124, z7 =0.022, z8 =0.142, z9 =0.138, z10=0.06.

Пример контрольного задания 3.

Необходимо передать сообщение: НЕУДОВЛЕТВОРИТЕЛЬНО с помощью алгоритма кодирования LZ77.

Пример контрольного задания 4.

Даны вероятности появления входных символов в канале и вероятности верной/ошибочной передачи: p(x0)=0.5, p(x1)=0.5, p(y0|x0)=1, p(y0|x1)=0.5, p(y1|x0)=0, p(y1|x1)=0.5.

Вычислить количество информации I(X,Y).

Тестовые задания

Пример тестового задания 1.

Формула условного распределения вероятностей. Свойство энтропии дискретного ансамбля. Формула условной энтропии при фиксированном событии. Свойства условной энтропии. Простая цепь Маркова. Энтропия на букву последовательности. Источник с памятью.

Пример тестового задания 2.

Неравенство Крафта. Код Гилберта-Мура. Двухпроходное побуквенное кодирование. Адаптивное кодирование. Адаптивное кодирование.

Пример тестового задания 3.

Характеристики архиваторов. Алгоритм LZW (LZ-78). Модели каналов. Симметричные каналы Типичные пары последовательностей Условная средняя взаимная информация.

Контрольная работа и тестовые задания оцениваются по 50-бальной шкале каждая.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью собеседования по экзаменационным билетам.

Для оценивания результатов обучения с помощью собеседования по экзаменационным билетам используются следующие показатели : владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач определения основных информационных характеристик источников сообщений и каналов связи.

КИМ формируется из трех теоретических вопросов и одной практической задачи.

Перечень вопросов к экзамену

Дискретные источники сообщений. Измерение информации. Собственная информация. Энтропия. Условная энтропия. Дискретные случайные последовательности. Цепи Маркова. Энтропия на сообщение дискретного стационарного источника. Равномерное кодирование дискретного источника. Постановка задачи. Неравенство Чебышева. Закон больших чисел. Прямая теорема кодирования для дискретного постоянного источника. Обратная теорема кодирования для дискретного постоянного источника. Множество типичных последовательностей для дискретного постоянного источника. Источники с памятью. Постановка задачи неравномерного побуквенного кодирования. Неравенство Крафта. Теоремы побуквенного неравномерного кодирования. Код Хаффмена. Избыточность кода Хаффмена. Код Шеннона. Код Гилберта-Мура. Неравномерное кодирование для стационарного источника. Постановка задачи универсального кодирования источников. Несколько полезных комбинаторных формул. Двухпроходное побуквенное кодирование. Нумерационное кодирование. Асимптотические границы избыточности универсального кодирования. Адаптивное кодирование. Сравнение алгоритмов. Монотонные коды. Интервальное кодирование и метод «стопка книг». Метод скользящего словаря (LZ-77). Алгоритм LZW (LZ-78). Предсказание по частичному совпадению. Сжатие с использованием преобразования Барроуза-Уилера. Сравнение способов кодирования. Характеристики архиваторов. Постановка задачи помехоустойчивого кодирования. Модели каналов. Взаимная информация. Средняя взаимная информация. Условная средняя взаимная информация. Теорема о переработке информации. Выпуклость средней взаимной информации. Информационная емкость и пропускная способность. Неравенство Фано. Обратная теорема кодирования. Вычисление информационной емкости. каналов без памяти. Симметричные каналы . Прямая теорема кодирования для дискретных постоянных каналов. Типичные пары последовательностей.