Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.1 Теория информации»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2022

Рабочая программа дисциплины «*Б1.Д.В.1 Теория информации*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "14" марта 2022 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнители:
ст. преподаватель кафедры КБМОИС *должность* *подпись* Н.А. Заельская *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Бигалиева *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 140757

© Заельская Н.А., 2022
© ОГУ, 2022

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:
изучение методов решения задач, связанных с процессами хранения и передачи информации в управляющих системах. Применение алгоритмов постановки задачи неравномерного побуквенного кодирования, постановки задачи универсального кодирования и наиболее эффективные способы универсального кодирования источников – методы Зива-Лемпела, а также их использования при решении практических задач.

Задачи:

- приобретение обучающимися знаний в области кодирования информации;
- получение представления о кодировании дискретных источников;
- получение студентами практических навыков при работе с алгоритмами кодирования источников.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика, Б1.Д.Б.44.4 Теория передачи сигналов и сообщений*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач	**Знать:** Технологию кодирования дискретных источников. **Уметь:** Вычислять теоретико-информационные характеристики источников сообщений. **Владеть:** Навыками применения математического аппарата для решения прикладных теоретико-информационных задач.
ПК*-2 Формирование требований в защите информации в автоматизированных системах	ПК*-2-В-1 Умеет определять угрозы безопасности информации, обрабатываемой автоматизированной системой	**Знать:** Основные тенденции современного развития кодирования дискретных источников. **Уметь:** Решать задачи кодирования и декодирования. **Владеть:** Способностью к обобщению, анализу алгоритмов кодирования информации, постановке цели и задачи кодирования.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**69,25**	**69,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**74,75**	**74,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в теорию информации.	3	1	-	-	2
2	Дискретные источники сообщений.	5	1	-	-	4
3	Измерение информации. Собственная информация. Энтропия.	6	2	-	-	4
4	Энтропия. Условная энтропия.	6	2		-	4
5	Дискретные случайные последовательности.	6	2	-	-	4
6	Энтропия на сообщение дискретного стационарного источника.	6	2	-	-	4
7	Равномерное кодирование дискретного источника. Постановка задачи.	6	2	-	-	4
8	Постановка задачи неравномерного побуквенного кодирования.	6	2	-	-	4
9	Неравенство Крафта.	6	2	-	-	4
10	Оптимальный побуквенный код Хаффмана.	8	2	-	2	4
11	Код Шеннона.	8	2	-	2	4
12	Код Гилберта-Мура.	8	2	-	2	4
13	Неравномерное кодирование для стационарного источника.	10	2	-	4	4
14	Кодирование дискретных источников при неизвестной статистике.	8,25	2	-	2,25	4
15	Монотонные коды.	5	1	-	2	2
16	Интервальное кодирование и метод «стопка книг».	5	1	-	2	2
17	Метод скользящего словаря (LZ-77).	12,25	2	-	4,25	6

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
18	Предсказание по частичному совпадению.	12,25	2	-	4,25	6
19	Сжатие с использованием преобразования Барроуза-Уилера	16,25	2	-	8,25	6
	Итого:	144	34	-	34	76
	Всего:	144	34	-	34	76

4.2 Содержание разделов дисциплины

1 Введение в теорию информации.

Наука теория информации. Задачи теории информации. Структурная схема типичной системы передачи и хранения информации. Разделы теории информации.

2 Дискретные источники сообщений.

Несовместные события. Совместно независимые события. Формула полной вероятности. Произведение множеств. Произведение вероятностных ансамблей. Условное распределение вероятностей на элементах множества. Математическое ожидание случайной величины.

3 Измерение информации. Собственная информация. Энтропия.

Задача количественного измерения информации. Сообщение как случайное событие. Интуитивные требования к информационной мере. Собственная информация. Свойства собственной информации.

4 Энтропия. Условная энтропия.

Энтропия дискретного ансамбля. Свойства энтропии. Статистическая зависимость сообщений. Последовательности зависимых сообщений. Условная собственная информация. Условная энтропия X при фиксированном элементе $y \in Y$. Условная энтропия ансамбля X при фиксированном ансамбле Y Свойства условной энтропии.

5 Дискретные случайные последовательности.

Случайные процессы. Задание случайного процесса. Предположение о стационарности. Стационарный процесс. Числовые характеристики стационарных процессов. Дискретный постоянный источник. Цепь Маркова связанности s. Однородная марковская цепь. Простая цепь Маркова. Матрица переходных вероятностей. Стационарное распределение для цепи Маркова. Финальное распределение вероятностей. Необходимое и достаточное условие эргодичности виде теоремы.

6 Энтропия на сообщение дискретного стационарного источника.

Два подхода к анализу информативности стационарного источника. Одномерная энтропия источника. n-мерная энтропия источника. Энтропия на букву последовательности длинны n. Теорема устанавливающая некоторые свойства двух информационных мер $H_n(X)$ и $H(X|X^{n-1})$ для стационарных источников.

7 Равномерное кодирование дискретного источника. Постановка задачи.

Кодовый алфавит. Кодовые слова. Равномерный код. Мощность кода. Скорость равномерного кода. Множество однозначно декодируемых последовательностей. Ошибка кодирования. Вероятность ошибки кодирования. Прямая теорема кодирования для дискретного постоянного источника. Обратная теорема кодирования для дискретного постоянного источника.

8 Постановка задачи неравномерного побуквенного кодирования.

Построение эффективного неравномерного двоичного кода над алфавитом A={a}. Свойство однозначной декодируемости. Неравномерный побуквенный код. Однозначно декодируемый код. Префиксный код. Кодовое дерево. Древовидный код. Средняя длина кодовых слов.

9 Неравенство Крафта.

Ограничения на длины кодовых слов. Формулировка теоремы в виде неравенства Крафта. Доказательство необходимости и достаточности. Формулировка теоремы справедливости неравенства Крафта для любых однозначно декодируемых кодов. Формулировка прямой теоремы побуквенного неравномерного кодирования. Формулировка обратной теоремы побуквенного неравномерного кодирования.

10 Оптимальный побуквенный код Хаффмана.

Свойства кодов. Алгоритм построения кодового дерева кода Хаффмана. Пример построения кода Хаффмана. Избыточность кода Хаффмана.

11 Код Шеннона.

Алгоритм построения кода Шеннона. Кодовое слово кода Шеннона. Пример построения кода Шеннона. Кодовое дерево кода Шеннона. Оценка средней длины кодовых слов. Графическая интерпретация кода Шеннона.

12 Код Гилберта-Мура.

Алгоритм построения кода Гилберта-Мура. Кодовое слово кода Гилберта-Мура. Пример построения кода Гилберта-Мура. Оценка средней длины кодовых слов. Графическая интерпретация кода Гилберта-Мура.

13 Неравномерное кодирование для стационарного источника.

Постановка задачи Неравномерное кодирование для стационарного источника. Средняя скорость кодирования для блоков длиной n. Обратная теорема неравномерного кодирования для стационарного источника. Прямая теорема неравномерного кодирования для стационарного источника. Арифметическое кодирование. Понятие лексикографического порядка. Вычисление кумулятивной вероятности. Рекуррентные формулы. Алгоритм арифметического кодирования. Графическая интерпретация арифметического кодирования. Алгоритм декодирования арифметического кода и некоторые аспекты практической реализации арифметического кодирования.

14 Кодирование дискретных источников при неизвестной статистике.

Постановка задачи универсального кодирования источников. Избыточность кодирования. Ограничения на множество допустимых алгоритмов. Двухпроходное побуквенное кодирование. Регулярный код Хаффмена.

15 Монотонные коды.

Простые методы универсального кодирования. Унарный код. Код Голомба. Код Галлагера-Ван Вухриса. Код Левенштейна. Упрощенный код Левенштейна (код Элайеса). Теорема о роли монотонных кодов в универсальном кодировании источников.

16 Интервальное кодирование и метод «стопка книг».

Интервальное кодирование. Метод «стопка книг». Теорема верхней оценки вредней скорости интервального кодирования.

17 Метод скользящего словаря (LZ-77).

Формальное описание алгоритма скользящего словаря (LZ-77). Окно наблюдения (Объем скользящего словаря). Алгоритм работы кодера. Пример алгоритма LZ-77. Модификация LZ-77, предложенная Фиала и Гриине (LZFG). Алгоритм LZFG. Алгоритм LZW. Практические аспекты применения алгоритма скользящего словаря.

18 Предсказание по частичному совпадению.

Метод кодирования PPM. Схема алгоритма PPM. Варианты алгоритма PPM. Идея алгоритма PPM. Практическая реализация алгоритма PPM.

19 Сжатие с использованием преобразования Барроуза-Уилера.

Прямое преобразование Барроуза-Уилера. Пример использования алгоритма PPMD. Результаты преобразования. Обратное преобразование Барроуза-Уилера.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	10	Реализация алгоритма построения кодового дерева – кода Хаффмена.	2
2	11	Реализация алгоритма построения кода Шеннона.	2
3	12	Реализация алгоритма построения кода Гилберта-Мура.	2
4	13	Реализация алгоритма Арифметического кодирования.	2
5	13	Реализация алгоритма декодирования Арифметического кода.	2
6	14	Реализация регулярного неравномерного кода. Регулярный код Хафмена.	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
7	15-16	Сравнение алгоритмов монотонного кодирования	4
8	17	Реализация метода скользящего словаря LZ-77(модификации метода - алгоритма LZFG).	4
9	18	Реализация алгоритма PPM	4
10	19	Прямое преобразование Барроуза-Уилера.	4
11	19	Обратное преобразование Барроуза-Уилера.	4
12	14, 17, 18, 19	Сравнение способов кодирования.	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Балюкевич Э. Л. Основы теории информации. Учебно-практическое пособие/ Балюкевич Э. Л. - Евразийский открытый институт, 2008. Университетская библиотека. Режим доступа - https://biblioclub.ru/index.php?page=book_red&id=90955.

2 Гультяева Т. А. Основы теории информации и криптографии. Конспект лекций / Новосибирск: НГТУ, 2010. Режим доступа – http://biblioclub.ru/index.php?page=book&id=228963.

5.2 Дополнительная литература

1 Игнатов, В. А. Теория информации и передачи сигналов: учеб. для вузов / В. А. Игнатов.- 2-е изд., перераб. и доп. - М. : Радио и связь, 1991. - 280 с.

2 Орлов, В. А. Теория информации в упражнениях и задачах: учеб. пособие для вузов / В. А. Орлов, Л. И. Филиппов. - М. : Высш. шк., 1976. - 136 с.

3 Новак, В. Математические принципы нечеткой логики: пер. с англ. / В. Новак, И. Перфильева, И. Мочкорж. - М. : Физматлит, 2006. - 352 с.

5.3 Периодические издания

1 Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать", 2022.

2 Информационные технологии: журнал. - М.: Агентство "Роспечать", 2022.

5.4 Интернет-ресурсы

www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;

www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»;

https://www.lektorium.tv/course/26243 - «Лекториум», МООК: «Введение в теорию информации».

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1 Операционная система Microsoft Windows текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cf-e05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8

2 Офисный пакет Microsoft Office (Word, Excel, Power Point) текущей версии. Доступен в рамках лицензионного соглашения OVS-ES. Разработчик: компания Microsoft. Режим доступа: https://products.office.com/en/home.

3 Теория информации [Электронный ресурс]: электронный курс в системе Moodle / Н.А. Заельская, Оренб. гос. ун-т. – Электрон. дан. – Оренбург: ОГУ.– Режим доступа: Электронные курсы ОГУ в системе обучения moodle. – https://moodle.osu.ru/course/view.php?id=935.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс оснащенный комплектами ученической мебели, доской и компьютерами с обеспечением доступа в электронную информационно-образовательную среду ОГУ.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой, с обеспечением доступа в электронную информационно-образовательную среду ОГУ.