

Государственное образовательное учреждение
«Приднестровский государственный университет им. Т.Г. Шевченко»

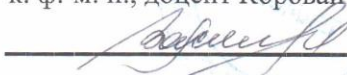
Физико-математический факультет

Кафедра прикладной математики и информатики

УТВЕРЖДАЮ

Декан физико-математического факультета

к. ф.-м. н., доцент Коровай О.В.



“12” 09 2018 г.

РАБОЧАЯ ПРОГРАММА

на 2018/2019 учебный год

2017 год набора

учебной дисциплины

«Алгоритмы дискретной математики»

Направление подготовки

01.03.04 «Прикладная математика»

Профиль

Математическое моделирование в экономике и технике

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Тирасполь 2018

Рабочая программа дисциплины «Алгоритмы дискретной математики» /составитель Е.В. Калинкова/ – Тирасполь: ГОУ «ПГУ им. Т.Г. Шевченко», 2018 – 10 с.

Рабочая программа предназначена для преподавания обязательной дисциплины вариативной части Блока 1 студентам очной формы обучения по направлению подготовки 01.03.04 – Прикладная математика.

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 01.03.04 – Прикладная математика (уровень бакалавриата), утвержденного приказом № 208 от 12.03.2015 Министерством образования и науки РФ.

Составитель  / Е.В. Калинкова, старший преподаватель/

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Алгоритмы дискретной математики» является изучение студентами комбинаторных алгоритмов, основ теории кодирования, сжатия и криптографической защиты информации.

Задачи изучения дисциплины:

- изучение и компьютерная реализация алгоритмов генерации комбинаторных объектов;
- овладение фундаментальными знаниями по теории кодирования;
- овладение технологиями кодирования и сжатия, восстановления и хранения информации;
- приобретение практических навыков реализации кодирующих и декодирующих алгоритмов;
- приобретение знаний в области криптографической защиты информации;
- формирование общекультурных и профессиональных компетенций, необходимых для осуществления профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО БАКАЛАВРИАТА

Дисциплина «Алгоритмы дискретной математики» относится к обязательным дисциплинам вариативной части Блока 1 (Б1.В.ОД.1).

Для освоения дисциплины «Алгоритмы дискретной математики» обучающиеся используют знания, умения и навыки, сформированные в ходе изучения дисциплин «Программирование для ЭВМ», «Линейная алгебра и аналитическая геометрия», «Дополнительные главы алгебры».

Дисциплина «Алгоритмы дискретной математики» является предшествующей для изучения дисциплины «Методы и средства защиты компьютерной информации».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование следующих компетенций:

Код компетенции	Формулировка компетенции
ОК-7	способность к самоорганизации и самообразованию
ОПК-1	готовность к самостоятельной работе
ОПК-2	способность использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии программирования
ПК-1	способность использовать стандартные пакеты прикладных программ для решения практических задач на электронных вычислительных машинах, отлаживать, тестировать прикладное программное обеспечение
ПК-3	способность и готовность демонстрировать знания современных языков программирования, операционных систем, офисных приложений, информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), способов и механизмов управления данными, принципов организации, состава и схемы работы операционных систем
ПК-10	готовность применять математический аппарат для решения поставленных задач, способность применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов
ПК-12	способность самостоятельно изучать новые разделы фундаментальных наук

В результате освоения дисциплины студент должен:

3.1. Знать:

- основные понятия комбинаторики;
- алгоритмы генерации основных комбинаторных объектов;
- основные понятия и теоремы теории кодирования;
- основные принципы и способы кодирования и декодирования;
- характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования;
- методы исследования кодов и их применений в ЭВМ и системах защиты информации;
- основные классы кодов, их параметры и алгоритмы кодирования/декодирования;
- основные методы криптографической защиты информации.

3.2. Уметь:

- реализовывать алгоритмы генерирования основных комбинаторных объектов;
- кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость;
- выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач;
- применять современные методы криптографической защиты информации.

3.3. Владеть:

- основными методами кодирования/декодирования и криптографической защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение трудоемкости в з.е./часах по видам аудиторной и самостоятельной работы студентов по семестрам

Семестр	Количество часов						Форма итогового контроля
	Трудо- емкость, з.е./часы	В том числе					
		Аудиторных				Самост. работы	
		Всего	Лекций	Лаб. раб.	Практич. зан.		
4	3/108	54	27		27	18	экзамен/36
Итого:	3/108	54	27		27	18	36

4.2. Распределение видов учебной работы и их трудоемкости по разделам дисциплины

№ раз- дела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеауд. работа (СР)
			Л	ПЗ	ЛР	
1	Комбинаторные алгоритмы.	10	4	4		2
2	Элементы теории кодирования.	14	6	4		4
3	Сжатие информации.	22	8	8		6
4	Основы теории помехоустойчивого кодирования.	15	6	6		3
5	Основы криптографии.	11	3	5		3
Итого:		72	27	27		18

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно- наглядные пособия
1	1	2	Генерация перестановок, сочетаний, размещений.	Презентация
2		2	Генерация подмножеств. Код Грея.	Презентация
3	2	2	Основные понятия теории кодирования. Алфавитное кодирование.	Презентация
4		2	Информационная энтропия. Цена кодирования. Метод кодирования Шеннона-Фано.	Презентация
5		2	Метод кодирования Хаффмана. Блочное кодирование.	Презентация
6	3	2	Понятие сжатия данных. Классификация алгоритмов сжатия. Алгоритмы энтропийного сжатия.	Презентация
7		2	Поточные и словарные алгоритмы сжатия. Преобразования: BWT, MTF.	Презентация
8		2	Алгоритмы сжатия изображений.	Презентация
9		2	Сжатие мультимедиа.	Презентация
10	4	2	Постановка задачи помехоустойчивого кодирования. Классификация помехоустойчивых кодов. Основные параметры корректирующих кодов.	Презентация
11		2	Коды с проверкой на четность. Линейные групповые коды. Порождающая матрица.	Презентация
12		2	Код Хэмминга Циклические коды.	Презентация
13	5	2	Основные понятия и задачи криптографии. Классификация шифров. Симметричные шифры.	Презентация
14		1	Асимметричные криптографические системы.	Презентация
Итого:		27		

Практические работы

№ п/п	Номер раздела дисциплины	Объем часов	Тема лабораторного занятия	Наимено- вание лабора- тории	Учебно- наглядные пособия
1	1	4	Генерация комбинаторных объектов.	КУВТ	метод. пособие
2	2	2	Алфавитное кодирование. Разделимые схемы.	КУВТ	метод. пособие
3		2	Кодирование с минимальной избыточностью.	КУВТ	метод. пособие
4	3	4	Сжатие данных без потерь.	КУВТ	метод. пособие
5		4	Сжатие графической информации.	КУВТ	метод. пособие
6	4	4	Код Хэмминга.	КУВТ	метод. пособие
7		2	Циклические коды.	КУВТ	метод. пособие
8	5	2	Симметричные шифры.	КУВТ	метод. пособие
9		3	Шифр RSA.	КУВТ	метод. пособие
Итого:		27			

Самостоятельная работа студента

Раздел дисциплины	№ п/п	Тема и вид СРС	Трудоемкость (в часах)
1	1	Генерация перестановок, сочетаний, размещений. (1,2,3)	1
	2	Генерация множества всех подмножеств. Генерация кодов Грея. (1,2)	1
2	3	Основные понятия и задачи теории кодирования. Алфавитное кодирование. Разделимые схемы. Префиксные и суффиксные схемы. Неравенство Макмиллана. (1,2,3)	2
	4	Цена кодирования. Оптимальное кодирование. Метод кодирования Шеннона-Фано. Метод кодирования Хаффмана. Блочное кодирование. (1,2,3)	2
3	5	Сжатие данных. Основные понятия. Классификация алгоритмов сжатия. Арифметическое кодирование. Кодирование длин серий. (1,2,3)	1
	6	Словарное сжатие. Алгоритм LZW. Преобразования: BWT, MTF. (1,2,3)	2
	7	Подходы к сжатию изображений. Стандарт сжатия изображений JPEG. Стандарт сжатия изображений JPEG-2000. Фрактальное сжатие изображений. (1,2)	2
	8	Подходы к сжатию видео. Особенности стандарта сжатия MPEG. Подходы к сжатию звука. Универсальные приемы сжатия звука. Сжатие звука по методу MP3. (1)	1
4	9	Постановка задачи помехоустойчивого кодирования. Классификация помехоустойчивых кодов. Основные параметры корректирующих кодов. (1,2,3)	1
	10	Коды с проверкой на четность. Линейные групповые коды. Порождающая матрица. (1,2,3)	1
	11	Код Хэмминга. Циклические коды. (1,2,3)	1
5	12	Основные понятия и задачи криптографии. Классификация шифровых систем. Симметричные шифры. (1,2,3)	1
	13	Основы асимметричных систем. Процедура открытого распределения ключей. Криптосистема RSA. Электронная цифровая подпись. (1,2,3)	2
Итого:			18

Примечание:

1 – проработка учебного материала (по конспектам лекций, учебной и научной литературе);

2 – подготовка к практической работе и оформление отчета;

3 – подготовка к контрольной работе.

5. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ)

По данной дисциплине курсовые проекты не предусмотрены.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: информационная лекция, проблемная лекция, лекция-беседа, лекция-визуализация, лабораторная работа с использованием активных и интерактивных форм проведения занятий.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Результаты освоения учебной дисциплины (модуля) оцениваются следующими средствами *текущего контроля* успеваемости:

- выполнение практических работ;
- оформление и защита практических работ;
- выполнение контрольных работ.

Методическое обеспечение текущего контроля:

1. Методические указания к выполнению практических работ.
2. Перечень вопросов по темам курса.

Отчет о выполненной практической работе оформляется каждым студентом индивидуально. Защита практических работ производится по каждой работе в отдельности в виде индивидуального собеседования с каждым студентом по теоретической и практической частям выполненной работы.

Промежуточная аттестация по итогам освоения дисциплины проводится в форме экзамена.

Перечень вопросов к экзамену

1. Генерация перестановок.
2. Генерация сочетаний.
3. Генерация размещений.
4. Генерация всех подмножеств множества.
5. Коды Грея и алгоритм их генерации.
6. Теории кодирования. Основные понятия и задачи.
7. Алфавитное кодирование. Основные понятия, схема алфавитного кодирования.
8. Разделимые схемы. Префиксные и суффиксные схемы. Неравенство Макмиллана.
9. Цена кодирования. Оптимальное кодирование.
10. Метод кодирования Шеннона-Фано.
11. Метод кодирования Хаффмана.
12. Блочное кодирование.
13. Сжатие данных. Основные понятия. Классификация алгоритмов сжатия.
14. Арифметическое кодирование.
15. Кодирование длин серий.
16. Словарное сжатие. Алгоритм LZW.
17. Преобразование BWT.
18. Преобразование MTF.
19. Направления сжатия изображений без потерь и с потерями качества.
20. Стандарт сжатия изображений JPEG.
21. Стандарт сжатия изображений JPEG-2000.
22. Фрактальное сжатие изображений.
23. Подходы к сжатию видео. Особенности стандарта сжатия MPEG.
24. Подходы к сжатию звука. Универсальные приемы сжатия звука. Сжатие звука по методу MP3.
25. Постановка задачи помехоустойчивого кодирования. Классификация помехоустойчивых кодов.
26. Общие принципы использования избыточности. Основные параметры корректирующих кодов.
27. Коды с проверкой на четность.
28. Линейные групповые коды. Порождающая матрица. Связь между порождающей и проверочной матрицами.

29. Код Хэмминга.
30. Циклические коды.
31. Криптография. Основные понятия и задачи. Классификация шифровых систем.
32. Симметричные шифры.
33. Основы асимметричных систем.
34. Процедура открытого распределения ключей.
35. Криптосистема RSA.
36. Электронная цифровая подпись.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература:

1. Новиков Ф.А. Дискретная математика для программистов: Учебник для вузов. 3-е изд. – СПб.: Питер, 2009. – 384 с.
2. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.
3. Д. Сэломон. Сжатие данных, изображений и звука. Москва: Техносфера, 2004. – 368 с.
4. М. Вернер. Основы кодирования. Учебник для ВУЗов. Москва: Техносфера, 2004 – 288 с.
5. Алферов А. П., Зубов А. Ю., Кузьмин А.С. , Черемушкин А. В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005. – 480 с.

8.2. Дополнительная литература:

1. Окулов С. М. Программирование в алгоритмах [Электронный ресурс] / С. М. Окулов. – 5-е изд. (эл.). – М.: БИНОМ. Лаборатория знаний, 2014. – 383 с.
2. Иванов Б.Н. Дискретная математика. Алгоритмы и программы: Учеб. Пособие / Б.Н. Иванов. – М.: Лаборатория Базовых Знаний, 2003. – 288 с.
3. Березкин Е.Ф. Основы теории информации и кодирования: Учебное пособие. – М.: НИЯУ МИФИ, 2010. – 312 с.
4. М.Н. Аршинов, Л.Е. Садовский. Коды и математика (рассказы о кодировании). – М.: Наука, Главная редакция физико-математической литературы, 1983. – 144 с. (Библиотека «Квант». Вып. 30).
5. Дориченко С.А., Яценко В.В. 25 этюдов о шифрах. – М.: ТЕИС, 1994. – 69 с.

8.3. Программное обеспечение и Интернет-ресурсы

1. Комбинаторика и переборные задачи. [Электронный ресурс]
URL: <http://algotlist.manual.ru/maths/combinat/index.php>
2. Булычев В.А. Методы программирования: переборные алгоритмы. [Электронный ресурс]
URL: <http://algotlist.manual.ru/maths/combinat/sequential.php>
3. Все о сжатии данных, изображений и видео. [Электронный ресурс]
URL: <http://www.compression.ru/book>
4. Методы сжатия изображений. [Электронный ресурс]
URL: <http://tik-diit.dp.ua/m312/>
5. Сжатие видео и звука. [Электронный ресурс]
URL: <http://tik-diit.dp.ua/m313/>
6. Основы помехозащитного кодирования. [Электронный ресурс]
URL: <https://tik-diit.dp.ua/m347/>
7. Основы криптографии. [Электронный ресурс]
URL: <https://www.intuit.ru/studies/courses/691/547/info>
8. Алгоритм шифрования RSA
URL: <https://www.youtube.com/watch?v=vooHjWxmclE>
URL: <https://ru.wikipedia.org/wiki/RSA>

8.4. Методические указания и материалы по видам занятий

1. В.В. Лидовский. Теория информации. [Электронный ресурс]: Московский центр непрерывного математического образования. URL: http://www.mccme.ru/free-books/izdano/2004/it_ebook1.pdf
2. А. И. Музыкантский, В. В. Фурин. Лекции по криптографии. [Электронный ресурс]: Московский центр непрерывного математического образования. URL: <https://www.mccme.ru/free-books/izdano/2013/crypto-2013.pdf>
3. Зверева Е.Н., Лебедько Е.Г. Сборник примеров и задач по основам теории информации и кодирования сообщений. – СПб: НИУ ИТМО, 2014. – 76 с. URL: <https://books.ifmo.ru/file/pdf/1576.pdf>

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Реализация данной учебной дисциплины осуществляется с использованием материально-технической базы, обеспечивающей проведение всех видов учебных занятий, предусмотренных программой учебной дисциплины и соответствующей действующим санитарным и противопожарным правилам и нормам.

Компьютерные классы оснащены современными персональными компьютерами и программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест достаточно, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.

Аудитория	Технические характеристики	На текущий момент
Аудитория 222	Локальная сеть (общеуниверситетская) Интернет Стандартное программное обеспечение для курсов, читаемых преподавателями кафедры ПМИИ	1 сервер 12 рабочих станций Интерактивная проекционная система (мультимедийный проектор и интерактивная доска)

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Данный курс предполагает овладение студентами основными методами кодирования, сжатия, восстановления и криптографической защиты информации, приобретение практических навыков реализации кодирующих и декодирующих алгоритмов.

Различные виды учебных занятий: лекции, практические занятия – тесно связаны друг с другом. Поэтому их пропуски, невыполнение или неусвоение требуют компенсации путем самостоятельной работы с использованием конспектов других студентов или рекомендованной литературы. В случае необходимости обращаться к преподавателю за консультацией.

Студентам рекомендуется посещать все занятия и вести подробный конспект; работать с основной и дополнительной литературой, пользоваться Интернет-ресурсами. Лекционный материал следует прорабатывать по конспектам и учебным пособиям после аудиторных занятий. Подготовка к практическим занятиям заключается в предварительном изучении соответствующего теоретического материала по конспекту лекций или по рекомендованной литературе.

Рабочая учебная программа по дисциплине «Алгоритмы дискретной математики» составлена в соответствии с требованиями федерального государственного образовательного стандарта ВО по направлению 01.03.04 «Прикладная математика» и учебного плана по профилю подготовки «Математическое моделирование в экономике и технике».

11. ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

Курс 2 группа ФМ17ДР62ПМ1 (210) семестр 4

Преподаватель-лектор

ст. преподаватель Калинкова Е.В.

Преподаватель, ведущий лабораторные занятия

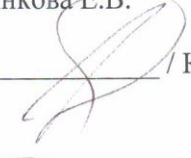
ст. преподаватель Калинкова Е.В.

Кафедра Прикладной математики и информатики

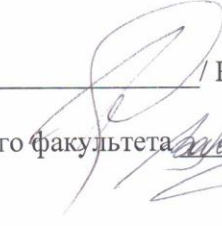
Семестр	Количество часов						Форма итогового контроля
	Трудо- емкость, з.е./часы	В том числе					
		Аудиторных				Самост. работы	
		Всего	Лекций	Лаб. раб.	Практич. зан.		
4	3/108	54	27		27	18	экзамен/36

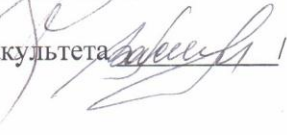
Форма текущей аттестации	Расшифровка	Минималь ное кол-во баллов	Максималь ное ко-во баллов
Посещение лекционных занятий		0	10
Выполнение и защита практических работ	За каждую практическую работу №1-№9 – 4 балла	0	36
Контрольная работа № 1		0	8
Контрольная работа № 2		0	8
Контрольная работа № 3		0	8
Итого количество баллов по текущей аттестации:		45	70
Промежуточная аттестация	экзамен	10	30
Итого по дисциплине:		55	100

Составитель  / Калинкова Е.В.

Зав. кафедрой (обслуживающей дисциплину)  / Коровай А.В., доцент, к. ф.-м. наук

Согласовано:

1. Зав. выпускающей кафедрой  / Коровай А.В., доцент, к. ф.-м. наук

2. Декан физико-математического факультета  / Коровай О.В., доцент, к. ф.-м. наук