Минобрнауки России

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

Кафедра математики и цифровых технологий

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.6 Теоретическая информатика»

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки
09.04.02 Информационные системы и технологии
(код и наименование направления подготовки)

Искусственный интеллект в промышленности
(наименование направленности (профиля) образовательной программы)

Квалификация
Магистр

Форма обучения
Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.Б.6 Теоретическая информатика*» рассмотрена и утверждена на заседании кафедры

Кафедра математики и цифровых технологий
наименование кафедры

протокол № 6 от 19 февраля 2024 г.

Заведующий кафедрой
Кафедра математики и цифровых технологий _____ А.Е. Шухман
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры МЦТ _____ Э. Ф. Морковина
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.04.02 Информационные системы и технологии _____ И.П. Болодурина
код наименование *личная подпись* *расшифровка подписи*

Научный руководитель магистерской программы _____ И.П. Болодурина
личная подпись *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
_____ Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
_____ И. В. Крючкова
личная подпись

№ регистрации _____

2

1 Цели и задачи освоения дисциплины

Формирование знаний о технологиях и методах управления программными проектами для достижения оптимального качества при минимуме затрат в процессе реализации успешного функционирования современных фирм и предприятий.

Задачи:

1) обучить основным принципам разработки программного обеспечения (ПО);

2) овладеть надежными методами реализации полного цикла разработки программного обеспечения;

3) обучить стандартам, гарантирующие соответствие процессов разработки ПО определенным характеристикам сертификации;

4) обладать навыками по управлению персоналом, продуктами и процессами;

5) обучить применять современные методы и средства программирования, основанные на использовании процедурного и объектно-ориентированного методов, при самостоятельной разработке программных продуктов для различных предметных областей

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.5 Математические основы машинного обучения*

Постреквизиты дисциплины: *Б1.Д.В.4 Машинное обучение, Б1.Д.В.6 Глубокое обучение, Б1.Д.В.Э.1.1 Компьютерная лингвистика, Б1.Д.В.Э.1.2 Поддержка принятия решений в промышленности, Б2.П.Б.У.1 Ознакомительная практика*

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
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2-В-1 Разрабатывает и реализует алгоритмы и программы обработки различных структур данных ОПК-2-В-2 Оценивает эффективность алгоритмов обработки структур данных	**Знать:** методы теоретической информатики для решения практических задач; алгоритмы эффективного, помехозащищенного и криптографического кодирования. **Уметь:** определять опасность и угрозы, возникающие в процессе получения, хранения и обработки информации; решать прикладные задачи теории информации на базе языков программирования и пакетов прикладных программ. **Владеть:** навыками использование математических и вычислительных моделей процессов передачи, хранения и преобразования информации, их оптимизация и выработка направлений совершенствования.
ОПК-5 Способен	ОПК-5-В-1	**Знать:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	Разрабатывает программное обеспечение информационных и автоматизированных систем	основные возможности современных информационно-коммуникационных технологий для оптимизации информационных систем с учетом требований информационной безопасности. **Уметь:** проводить анализ информационных систем и процессов с учетом требований информационной безопасности. **Владеть:** способностью самостоятельно получать знания при решении нестандартных задач профессиональной деятельности с учетом требований информационной безопасности.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	2 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**35,25**	**35,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
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;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**108,75**	**108,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 1 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Теоретико-числовые алгоритмы	72	9	8		55
2	Криптографические алгоритмы	72	9	8		55
	Итого:	144	18	16		110
	Всего:	144	18	16		110

4.2 Содержание разделов дисциплины

1. Теоретико-числовые алгоритмы

Предварительные сведения из теории чисел (полная и приведенная системы вычетов, теорема Вильсона, малая теорема Ферма, функция и теорема Эйлера, китайская теорема об остатках, алгоритм Гарнера, квадратичные вычеты, символы Лежандра и Якоби, показатель числа по модулю, первообразный корень).

Проверка чисел на простоту (тест на основе МТФ, тесты Соловея-Штрассена, Рабина-Миллера и Миллера, числа Кармайкла).

Доказательство простоты и построение больших простых чисел (n-1 и n+1 методы, метод Маурера, алгоритм Агравала-Кайала-Саксены)

Дискретное логарифмирование (шаг младенца-шаг великана, алгоритм Полига-Хеллмана, алгоритм исчисления порядка).

Факторизация целых чисел (метод Ферма, метод Шермана-Лемана, ро-метод Полларда, алгоритм Полларда-Штрассена, метод Диксона).

2. Криптографические алгоритмы

Простейшие криптосистемы и их взлом (Сцитала, шифр Цезаря, квадрат Виженера, шифр Вернама, Энигма).

Схема Диффи-Хеллмана, шифры Шамира и Эль-Гамаля, RSA, функция Рабина.

Электронные протоколы для популярных задач (разделение секрета, ставки, жребий, раздача карт, аутентификация, электронная подпись и т.д.).

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Математические основы криптографии	2
2	1	Проверка чисел на простоту	2
3	1	Построение больших простых чисел	2
4	1	Дискретное логарифмирование	2
5	1	Факторизация целых чисел	2
6	2	Простейшие криптосистемы и их взлом	2
7	2	Алгоритмы распределения ключей	2
8	2	Электронные криптографические протоколы	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Игошин, В.И. Математическая логика и теория алгоритмов [Текст]: учеб. пособие для вузов / В.И. Игошин. – 3-е изд., стер. – М.: Академия, 2008. – 448 с.
2. Судоплатов, С.В. Математическая логика и теория алгоритмов [Текст]: учебник / С.В. Судоплатов, Е.В. Овчинникова. – М.: ИНФРА-М, 2008. – 224 с.
3. Гохберг, Г.С. Информационные технологии [Текст]: учебник для использования в учебном процессе образовательных учреждений, реализующих программы государственного образовательного стандарта среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника" / Г.С. Гохберг, А.В. Зафиевский, А.А. Короткин. – 9-е изд., перераб. и доп. – Москва: Академия, 2014. – 235 с.: ил. – (Профессиональное образование. Информатика и вычислительная техника). – Библиогр.: с. 231. – ISBN 978-5-4468-0766-6.

5.2 Дополнительная литература

1. Алгоритмы: построение и анализ = Introduction to Algorithms [Текст] / Т. Кормен [и др.]; [пер. с англ. И.В. Красикова, Н.А. Ореховой, В.Н. Романова; под ред. И.В. Красикова]. – 2-е изд. – Москва; Санкт-Петербург; Киев: Вильямс, 2013. – 1296 с.: ил. – Парал. тит. л. англ. – Прил.: с. 1189-1256. – Библиогр.: с. 1257-1276. – Предм. указ.: с. 1277-1290. – ISBN 978-5-8459-0857-5. – ISBN 0-07-013151-1.
2. Макконелл, Дж. Анализ алгоритмов: Вводный курс: Пер. с англ. / Дж. Макконелл. – М.: Техносфера, 2002. – 304 с.
3. Кнут, Д.Э. Искусство программирования [Текст] / Д.Э. Кнут; под общ. ред. Ю.В. Козаченко. – 3-е изд. – Москва: Вильямс, 2012. Т. 1: Основные алгоритмы, 2012. – 713 с. – Прил.: с. 683-691. – Предм. имен. указ.: с. 692-712. – ISBN 978-5-8459-0080-7.

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство "Роспечать", 2018.
2. Информационные технологии: журнал. – М.: Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

1. http://www.citforum.ru/ – портал аналитических и научных статей в области информационных технологий
2. http://www.rsdn.ru – сайт Российской сети разработчиков ПО, содержит статьи по современным средствам программирования.
3. http://www.intuit.ru – сайт Интернет-университета информационных технологий, представляет учебные курсы по разным областям ИТ.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Обязательное ПО

1. Операционная система РЕД ОС для рабочих станций, имеется лицензия, входит в реестр отечественного ПО.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Система управления учебным процессом Moodle, свободно распространяемая.
4. Программная система для организации видео-конференц-связи MTS Link.
5. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.

Дополнительно

1. Система программирования Python, свободно распространяемая по лицензии PSFL.
2. Интегрированная среда разработки ПО NetBeans, свободно распространяемая по лицензии Apache.
3. Интегрированная среда разработки ПО VisualStudioCode, свободно распространяемая по лицензии MIT.
4. Система управления базами данных MySQL, свободно распространяемая по лицензии GPL.
5. Система программирования Oracle Java SEJDK, бесплатно распространяемая по лицензии Oracle Technology Network License.
6. Средства для разработки JetBrains All Products Pack, бесплатно лицензируемая для образовательного учреждения (включает C++, Java, C#, PHP, Python…)

БДиИПС

1. Elibrary[Электронный ресурс] : реферативная база данных, с ограниченным доступом к полным текстам статей – Режим доступа: https://www.elibrary.ru/, в локальной сети ОГУ.
2. Math-Net.ru[Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа http://www.mathnet.ru/.
3. Wolfram|Alpha[Электронный ресурс]:база знаний и справочная система, включающая множество вычислительных алгоритмов. – Режим доступа https://www.wolframalpha.com/
4. Большая Российская энциклопедия [Электронный ресурс]: универсальная энциклопедия, содержит статьи по всем областям знаний, справочники по персоналиям, словари. – жим доступаhttps://bigenc.ru/

6 Материально-техническое обеспечение дисциплины

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

Для проведения лабораторного практикума предназначена специализированная лаборатория кафедры. При выполнении лабораторных работ используются компьютеры Pentium4-3Гц/512Мб/80ГБ с 17-дюймовыми мониторами, объединенные в локальную сеть, подключенную через университетскую сеть к сети Интернет. Для чтения лекций используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Помещения для самостоятельной работы студентов оснащены компьютерной техникой, подключенной к сети Интернет. А также предоставляется доступ в электронную информационно-образовательную среду ОГУ.