Минобрнауки России

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

Кафедра геометрии и компьютерных наук

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.10 Теоретические основы информатики»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.02 Фундаментальная информатика и информационные технологии
(код и наименование направления подготовки)

Разработка и администрирование информационных систем
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2021

Рабочая программа дисциплины «*Б1.Д.В.10 Теоретические основы информатики*» рассмотрена и утверждена на заседании кафедры

Кафедра геометрии и компьютерных наук
наименование кафедры

протокол № 6 от 18.02.2021 г.

Заведующий кафедрой
Кафедра геометрии и компьютерных наук _____ А.Е. Шухман
наименование кафедры *подпись* *расшифровка подписи*

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

_____ _____ _____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.02 Фундаментальная информатика и информационные технологии
код наименование
_____ А.Е. Шухман
личная подпись *расшифровка подписи*

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

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

№ регистрации _____

2

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины:

Обеспечить теоретическую подготовку в области основ теории информации, рассмотреть основные понятия, вопросы измерения количества информации, историю развития вычислительной техники, основы формальной логики, теории алгоритмов, базовые понятия теории кодирования, защиты информации, а также обеспечить практическую подготовку владения компьютерными технологиями.

Задачи:

- сформировать представление о том, что такое информация;
- сформировать представление об основных свойствах принципах хранения, передачи, обработки и защиты информации;
- освоить основные методики обработки информации;
- получить представление о различных видах компьютерных технологий;
- сформировать практические навыки владения компьютерными технологиями для сбора, хранения и обработки информации.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.11 Основы информатики, Б1.Д.Б.18 Дискретная математика и математическая логика, Б1.Д.Б.23 Алгоритмы и анализ сложности*

Постреквизиты дисциплины: *Б1.Д.В.Э.2.1 Математические основы криптографии, Б1.Д.В.Э.2.2 Теория нечетких множеств, Б1.Д.В.Э.3.1 Теория кодирования, Б2.П.В.У.1 Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы), Б2.П.В.П.2 Научно-исследовательская работа*

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
ПК*-1 Способен проводить под научным руководством локальные исследования на основе существующих методов разработки и анализа алгоритмов, математического и компьютерного моделирования, анализа данных и машинного обучения в конкретной области профессиональной деятельности	ПК*-1-В-1 Решает научные задачи в связи с поставленной целью и в соответствии с выбранной методикой на основе существующих методов разработки и анализа алгоритмов, математического и компьютерного моделирования, анализа данных и машинного обучения ПК*-1-В-2 Подготавливает научные обзоры, публикации, рефераты и библиографии по тематике проводимых исследований на русском	**Знать:** об информации, методах ее хранения, обработки и передачи; о технических средствах обработки информации; о теоретических основах информатики как о научной дисциплине **Уметь:** представлять информацию в формализованном виде; измерять количество информации. **Владеть:** навыками разработки и анализа алгоритмов, навыками презентации на заданную тему по информационным технологиям.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	языке ПК*-1-В-3 Выступает с сообщениями и участвует в научных дискуссиях на семинарах и конференциях	
ПК*-2 Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, методы теоретической информатики, современные информационные технологии	ПК*-2-В-2 Применяет в профессиональной деятельности методы теоретической информатики	**Знать:** принципы организации ЭВМ; различные системы счисления; арифметические и логические основы ЭВМ; основные методы преобразования сигналов при передачи их по каналам связи **Уметь:** получать, хранить, обрабатывать, анализировать полученную из различных источников информацию; проводить анализ современной научной и учебной литературы. **Владеть:** навыками работы в различных программных системах.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**51,25**	**51,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**92,75**	**92,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Алгоритм: понятие, виды, формализация.	44	6	4	4	30
2	Эффективные алгоритмы обработки данных	50	6	6	6	32
3	Основы криптографии.	50	6	6	6	32
	Итого:	144	18	16	16	94
	Всего:	144	18	16	16	94

4.2 Содержание разделов дисциплины

1 Алгоритм: понятие, виды, формализация. Интуитивное понятие алгоритма. Свойства алгоритмов. Способы записи алгоритмов. Основные алгоритмические конструкции. Структурная теорема. Необходимость формализации понятия алгоритма. Вычислимые функции, тезис Черча. Простейшие функции. Операции суперпозиции, примитивной рекурсии и минимизации. Примитивно-рекурсивные, частично-рекурсивные и общерекурсивные функции. Вычислимость частично-рекурсивных функций. Рекурсивные и рекурсивно перечислимые множества, их свойства. Универсальная общерекурсивная функция. Машины Тьюринга: основные понятия, тезис Тьюринга. Примеры машин Тьюринга. Универсальная машина Тьюринга. Машина Поста. Алгоритмы преобразования слов. Нормальные алгоритмы Маркова. Подстановки. Схема алгоритма. Выполнение нормального алгоритма. Примеры нормальных алгоритмов. Алгоритмически неразрешимые проблемы.

2 Эффективные алгоритмы обработки данных. Понятие сложности алгоритма. Методы анализа рекурсивных алгоритмов. Классы сложности алгоритмов. Основы экспериментального исследования трудоемкости алгоритмов. Алгоритмическая сводимость проблем. Основы теории NP-полноты. Применение теории NP-полноты для анализа сложности проблем. Методы приближенного решения NP-полных задач: метод отжига, генетические и муравьиные алгоритмы.

3 Основы криптографии. Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, шифр Сцитала, решетка Кардано, книжный шифр. Основные этапы становления криптографии как науки. Симметричные и асимметричные криптосистемы. Предварительное распределение ключей. Схемы разделения секрета. Сертификация открытых ключей. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Шифры замены. Обобщенная модель шифра замены. Шифр гаммирования. Табличное и модульное гаммирование. Сеть Фейстеля. DES-алгоритм. Усложнения DES-алгоритма. Российский стандарт шифрования ГОСТ-28147. Различия между DES и ГОСТ. Шифр AES. Режимы блочного шифрования. Функции хеширования и целостность данных. Целостность данных и аутентификация сообщений. Системы шифрования с открытыми ключами. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Машины Тьюринга и Поста.	2
2	1	Нормальные алгоритмы Маркова.	2
3	2	Анализ алгоритмов.	2
4	2	Эффективные алгоритмы обработки данных	2
5	2	Методы решения NP-полных задач.	2
6	3	Алгоритмы симметричного шифрования	2
7	3	Алгоритмы ассиметричного шифрования	2
8	3	Электронная цифровая подпись	2
		Итого:	16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Формализация понятия алгоритма	4
2	2	Эффективные алгоритмы обработки данных	4
3	2	Методы решения NP-полных задач.	4
4	3	Алгоритмы симметричного и ассиметричного шифрования	4
		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. Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов [Текст] : учебное пособие для студентов вузов/ М. М. Глухов, А. Б. Шишков. - СПб. : Лань, 2012. - 416 с. - (Учебники для вузов. Специальная литература). - Библиогр.: с. 398-401. - ISBN 978-5-8114-1344-7.

4. Романьков, В. А. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-105918-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018899

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.

4. Криптографическая защита информации : учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2018. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-16-106001-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/901659

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

1. Операционная система Microsoft Windows, приобретенная по лицензии Microsoft DreamSpark Premium (для программ до 2018 г.), Azure Dev Tools for Teaching (для программ 2019 г.)
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО
4. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.
5. Система программирования MS Visual Studio, распространяемая по лицензии Microsoft DreamSpark Premium (для программ до 2018 г.), Azure Dev Tools for Teaching (для программ 2019 г.)
6. Система программирования Python, свободно распространяемая по лицензии PSFL.
7. SCOPUS [Электронный ресурс] : реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ.
8. Springer [Электронный ресурс] : база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH . – Режим доступа : https://link.springer.com/, в локальной сети ОГУ.
9. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа http://www.mathnet.ru/.
10. Wolfram|Alpha [Электронный ресурс]: база знаний и справочная система, включающая множество вычислительных алгоритмов. – Режим доступа https://www.wolframalpha.com/
11. CITforum.ru Аналитическая информация по всем областям компьютерной сферы (http://www.citforum.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 геометрии и компьютерных наук (ауд. № 1504а). 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.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.