МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Теория сложности алгоритмов

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Теория сложности алгоритмов» являются: закладка математического фундамента как средства изучения окружающего мира для успешного освоения дисциплин естественнонаучного и профессионального циклов; получение студентами основ теоретических знаний и прикладных навыков применения математических методов и моделей; подготовка к использованию этих методов для разработки и принятия эффективных организационных и управленческих решений на транспорте; построение и оценка математических алгоритмов для решения задач; применение полученных теоретических знаний на практике; оценка сложности реализации алгоритмов решения ЭВМ; развитие логического мышления и повышение общего уровня культуры студентов.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Уметь:

Применяет систему фундаментальных знании? (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации.

Уметь:

Применяет методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.

Уметь:

Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах.

Уметь:

Устанавливает причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям.

Уметь:

Анализирует корректность комбинаторных, теоретико-числовых и криптографических алгоритмов в современных программных комплексах.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №5
Контактная работа при проведении учебных занятий (всего):	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	34	34

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 112 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Раздел 1 Введение в сложность алгоритмов 1. Детерминированная машина Тьюринга. Схема машины Тьюринга: управляющее устройство, читающая/пишущая головка, лента. Определение ДМТ-программы. Примеры ДМТ-программ (программ для детерминированной машины Тьюринга). 2. Задачи и алгоритмы. Массовая и индивидуальная задача. Примеры. Определение алгоритма. Сложность решения задачи в наихудшем и наилучшем случаях. Труднорешаемые задачи. 3. Задачи распознавания, языки и кодирование. Сведение любой массовой задачи к задаче распознавания. Соответствие между задачами распознавания и языками. Язык, распознаваемой программой. Что значит, что программа решает задачу распознавания при кодировки.
2	Раздел 2 Класс языков и задач P 4. М-ДМТ программа с полиномиальными временем работы 5. Алгоритмы вычисления (X n-ой степени) mod m и n! 6. Поиск в упорядоченном массиве. 7. Сортировка. Сортировка слиянием. 8. Полиномиальные алгоритмы для задач дискретной математики. Минимальное остовное дерево. Кратчайший путь в графе. Алгоритм Прима. 9. Рекуррентные методы построения алгоритмов. Метод динамического программирования. Задача об оптимальном порядке умножения матриц. Алгоритм Карацубы для умножения чисел. Метод «разделяй и властвуй». 10. Алгоритмы решения логических задач. Задача об устойчивом бракосочетании. Задача об ханойских башнях. Задачи из дискретной математики. Определение входной длины и вычисление количества операций, временной сложности.
3	Раздел 3 Класс языков и задач NP 11. Понятие полиномиальной проверяемости. 12. Недетерминированная машина Тьюринга.13. М-НДМТ программа с полиномиальным временем работы. 14. Алгоритмы с экспоненциальной временной сложностью. 15. Соотношение классов P и NP. Раздел 4 Класс NP-полных задач. 16. Полиномиальная сводимость языков и её свойства. Полиномиальная эквивалентность языков и задач. 17. Теорема Кука и идея её доказательства. 18. 6 основных NP-полных задач Задачи КМ, ГЦ, КЛИКА, ВЫП, 3-ВЫП, 3-С и их соотношения в системе сводимости. 19. Возможные решения проблемы P=NP?

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	РАЗДЕЛ 1 Детерминированная машина Тьюринга.
2	РАЗДЕЛ 1 Задачи и алгоритмы
3	РАЗДЕЛ 1 Задачи распознавания, языки и кодирование.
4	РАЗДЕЛ 2 М-ДМТ программа с полиномиальными временем работы
5	РАЗДЕЛ 2 Алгоритмы вычисления x степени n mod m и n!
6	РАЗДЕЛ 2 Поиск в упорядоченном массиве
7	РАЗДЕЛ 2 Сортировка. Сортировка слиянием

№ п/п	Тематика практических занятий/краткое содержание
8	РАЗДЕЛ 2 Полиномиальные алгоритмы для задач дискретной математики
9	РАЗДЕЛ 2 Рекуррентные методы построения алгоритмов
10	РАЗДЕЛ 2 Метод динамического программирования
11	РАЗДЕЛ 2 Алгоритмы решения логических задач
12	РАЗДЕЛ 3 Понятие полиномиальной проверяемости. Недетерминированная машина Тьюринга.
13	РАЗДЕЛ 3 М-НДМТ программа с полиномиальным временем работы. Соотношение классов P и NP.
14	РАЗДЕЛ 3 Алгоритмы с экспоненциальной временной сложностью
15	РАЗДЕЛ 3 Полиномиальная сводимость языков и её свойства. Теорема Кука и идея её доказательства.
16	РАЗДЕЛ 3 6 основных NP-полных задач. Возможные решения проблемы P=NP?

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Написание ДМТ-программ. Нахождение сложности решения задачи в наихудшем и наилучшем случаях.
2	Поиск в массиве. Сортировка. Решение конкретных задач. Оценка каждого алгоритма, выбор оптимального. Написание программ, реализующих алгоритм. Рекуррентные методы построения алгоритмов. Проработка учебного материала по конспекту лекций. Решение задач с помощью изученных алгоритмов. Полиномиальные алгоритмы для задач дискретной математики. Решение задач. Написание программ, реализующих алгоритмы. Интересные логические задачи. Нахождение алгоритмов, решающих задачи.
3	Решение задач алгоритмами с экспоненциальной временной сложностью. Написание программ, реализующих алгоритм. Нахождение полиномиальной сводимости между задачами. Представление полиномиального алгоритма, сводящего одну задачу к другой. Проработка учебного материала по конспектам лекций и рекомендованной литературе. Рассмотрение индивидуальных задач из числа NP-полных.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Элементы теории сложности алгоритмов и вычислений В.Х. Хаханян; МИИТ. Каф. "Прикладная математика-2" Однотомное издание МИИТ , 2006	НТБ (фб.); НТБ (чз.2)
1	Теория алгоритмов учеб. пособие для студ. вузов Крупский В.Н., Плиско В.Е. Академия, , 2009	НТБ МИИТ
2	Задачи по теории множеств, математической логике и теории алгоритмов Лавров И.А., Максимова Л.Л. ФИЗМАТЛИТ , 2014	http://www.knigafund.ru/books/171881

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

http://miit-ief.ru/student/methodical_literature/ (Электронная библиотека ИЭФ) http://library.miit.ru (НТБ МИИТа (электронно-библиотечная система)) https://www.biblio-online.ru (Электронная библиотечная система «Юрайт», доступ для студентов и преподавателей РУТ(МИИТ)) http://e.lanbook.com (Электронно-библиотечная система «Лань», доступ для студентов и преподавателей РУТ(МИИТ) https://www.book.ru/ (ЭБС book.ru – доступ для преподавателей и студентов РУТ(МИИТ) https://www.ibooks.ru/ (ЭБС ibooks.ru – доступ для преподавателей и студентов РУТ(МИИТ) https://www.knigafund.ru/ (ЭБС Книгафонд – доступ для преподавателей и студентов ИЭФ РУТ(МИИТ)

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

При осуществлении образовательного процесса по дисциплине требуется наличие следующего ПО:OSWindows, Microsoft Office, система компьютерного тестирования АСТ. В образовательном процессе применяются следующие информационные технологии: персональные компьютеры; компьютерное тестирование; мультимедийное оборудование; средства коммуникаций: ЭИОС РУТ(МИИТ) и/или электронная почта.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для успешного проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования. Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Для организации самостоятельной работы студентов необходима аудитория с рабочими местами, обеспечивающими выход в Интернет. Необходим доступ каждого студента к информационным ресурсам – институтскому библиотечному фонду и сетевым ресурсам Интернет.

9. Форма промежуточной аттестации:

Экзамен в 5 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры «Управление и защита информации» Е.П. Балакина

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин