

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:

УТВЕРЖДАЮ:

Выпускающая кафедра ЦТУТП
Доцент

Директор ИУЦТ

05 октября 2020 г.

В.Е. Нутович

06 октября 2020 г.

С.П. Вакуленко



Кафедра «Математическое моделирование и системный анализ»

Автор Андреева Татьяна Владимировна, к.ф.-м.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Элементы теории алгоритмов и защита информации»

Направление подготовки:	01.03.02 – Прикладная математика и информатика
Профиль:	Математические модели в экономике и технике
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии Протокол № 3 05 октября 2020 г. Председатель учебно-методической комиссии</p> <p style="text-align: right;"> Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 6 27 апреля 2020 г. И.о. заведующего кафедрой</p> <p style="text-align: right;"> Г.А. Зверкина</p>
--	---

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Элементы теории алгоритмов и защита информации» является овладение базовыми понятиями, основными определениями и элементарными результатами теории алгоритмов, теории кодирования и криптографии.

Основной целью изучения учебной дисциплины «Элементы теории алгоритмов и защита информации» является формирование у обучающегося компетенций в области математики, необходимых при сборе, обработке и анализе информации; оценке эффективности проектов; подготовке отчетов для следующих видов деятельности: проектная и производственно-технологическая; научная и научно-исследовательская.

Дисциплина предназначена для получения знаний в решении следующих профессиональных задач (в соответствии с видами деятельности):

проектная и производственно-технологическая:

исследование математических методов моделирования информационных и имитационных моделей по тематике выполняемых научно-исследовательских прикладных задач или опытно-курсовых работ;

научная и научно-исследовательская:

исследование и разработка математических моделей, алгоритмов и методов по тематике проводимых научно-исследовательских проектов.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Элементы теории алгоритмов и защита информации" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК-7	способностью к самоорганизации и самообразованию
ОПК-1	способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой
ОПК-2	способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-2	способностью понимать, совершенствовать и применять современный математический аппарат

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме и являются традиционными классически-лекционными. Практические занятия организованы в традиционной классно-урочной организационной форме. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий. Самостоятельная работа студента организована с использованием традиционных видов работы. К ним относится отработка лекционного материала и отработка отдельных тем по учебным пособиям. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Проведение занятий по дисциплине возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников. В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости): - использование современных средств коммуникации; - электронная форма обмена материалами; - дистанционная форма групповых и индивидуальных консультаций; - использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Теория алгоритмов.

Тема: Понятие массовой задачи

Тема: Алгоритм, решающий массовую задачу. Свойства алгоритма

Тема: Машина Тьюринга

Тема: Тезис Тьюринга

Контрольная работа №1

Тема: Кодирование МТ. Проблема самоприменимости. Алгоритмически неразрешимые задачи

Тема: Универсальная МТ.

Тема: Понятие сложности алгоритма и сложности задачи. Полиномиальные алгоритмы.

Тема: Примеры "быстрых" алгоритмов

Тема: Недетерминированный алгоритм.

Тема: Классы задач

Устный опрос

Тема: Примеры NP-полных задач

по результатам контрольной работы №1 и устного опроса

РАЗДЕЛ 2

Теория кодирования.

Тема: Алфавитное кодирование. Однозначное кодирование

Тема: Коды с минимальной избыточностью

Тема: Коды с обнаружением и исправлением ошибок

Контрольная работа №2

РАЗДЕЛ 3

Криптография.

Тема: Основные задачи криптографии. Исторический очерк и примеры шифров.

Тема: Понятия алгоритма зашифрования, алгоритма расшифрования, ключа.
Классификация шифров. Открытые и закрытые ключи

Контрольная работа №3

Тема: Понятие односторонней функции. Шифрсистема RSA. Шифрсистема Эль-Гамала

тест

Тема: Криптографические протоколы. Криптографические хэш-функции

по результатам контрольных работа 2, 3 и теста

Экзамен