МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Выпускающая кафедра ЦТУТП	Директор ИУЦТ
Доцент	
В.Е. Нутович	С.П. Вакуленко
05 октября 2020 г.	06 октября 2020 г.

Кафедра «Математическое моделирование и системный анализ»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ 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

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии Протокол № 3 05 октября 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 6 27 апреля 2020 г. И.о. заведующего кафедрой Г.А. Зверкина

Москва 2020 г.

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 задача 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.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Математическая логика:

Знания: определения функции и формулы алгебры логики, основные правила комбинаторики, понятие мощности множества.

Умения: выполнять преобразования логических выражений.

Навыки: навыками доказательства теорем.

2.1.2. Основы информатики:

Знания: понятие алгоритма.

Умения: строить блок-схемы алгоритмов

Навыки: навыками описания и построения алгоритмов решения задач.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Компьютерная безопасность

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОК-7 способностью к самоорганизации и самообразованию	Знать и понимать: понятия, определения, термины Уметь: самостоятельно применять полученные знания в профессиональной деятельности, совершенствуя свои навыки и умения Владеть: навыками систематизировать, дифференцировать факты, методы, задачи и т.д., самостоятельно формулируя основания для классификации
2	ОПК-1 способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой	Знать и понимать: базовые объекты курса и связи между ними Уметь: формулировать, выдвигать гипотезы о причинах возникновения той или иной ситуации (состояния, события), о путях (тенденциях) ее развития и последствиях Владеть: навыками систематизировать, дифференцировать факты, методы, задачи
3	ОПК-2 способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии	Знать и понимать: методологические основы приобретения новых научных и профессиональных знаний Уметь: использовать современные образовательные и информационные технологии Владеть: приёмами и навыками работы с современными образовательными и информационными технологиями
4	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	Знать и понимать: понятия об информационном обществе и роли информационных технологий в жизни общества Уметь: выбирать методы, приемы, алгоритмы для решения задач курса с учетом основных требований информационной безопасности Владеть: навыками решения стандартных задач с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
5	ПК-2 способностью понимать, совершенствовать и применять современный математический аппарат	Знать и понимать: понятия, определения, термины; методы, алгоритмы, способы решения задач курса Уметь: вычислять, оценивать величины, используя известные методы, алгоритмы, законы, теории, закономерности Владеть: навыками описывать результаты,

№ п/п	Код и название компетенции	Ожидаемые результаты
		формулировать выводы

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 3
Контактная работа	56	56,15
Аудиторные занятия (всего):	56	56
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Контроль самостоятельной работы (КСР)	2	2
Самостоятельная работа (всего)	25	25
Экзамен (при наличии)	27	27
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

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

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	3	Раздел 1 Теория алгоритмов.	22		8/6	1	17	48/6	
2	3	Тема 1.1 Понятие массовой задачи	2					2	
3	3	Тема 1.2 Алгоритм, решающий массовую задачу. Свойства алгоритма	2					2	
4	3	Тема 1.3 Машина Тьюринга	2		2/2		5	9/2	
5	3	Тема 1.4 Тезис Тьюринга	2				2	4	, Контрольная работа №1
6	3	Тема 1.5 Кодирование МТ. Проблема самоприменимости. Алгоритмически неразрешимые задачи	2				3	5	
7	3	Тема 1.6 Универсальная МТ.	2					2	
8	3	Тема 1.7 Понятие сложности алгоритма и сложности задачи. Полиномиальные алгоритмы.	2		2/2	1		5/2	
9	3	Тема 1.8 Примеры "быстрых" алгоритмов	2		2		4	8	
10	3	Тема 1.9 Недетерминированный алгоритм.	2					2	
11	3	Тема 1.10 Классы задач	2					2	, Устный опрос
12	3	Тема 1.11 Примеры NP-полных задач	2		2/2		3	7/2	ПК1, по результатам контрольной работы №1 и устного опроса
13	3	Раздел 2 Теория кодирования.	6		4	1	3	14	
14	3	Тема 2.1 Алфавитное кодирование. Однозначное кодирование	2		2			4	
15	3	Тема 2.2 Коды с минимальной избыточностью	2		1	1		4	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
16	3	Тема 2.3 Коды с обнаружением и исправлением ошибок	2		1		3	6	, Контрольная работа №2
17	3	Раздел 3 Криптография.	8		6		5	19	
18	3	Тема 3.1 Основные задачи криптографии. Исторический очерк и примеры шифров.	2		2			4	
19	3	Тема 3.2 Понятия алгоритма зашифрования, алгоритма расшифрования, ключа. Классификация шифров. Открытые и закрытые ключи	2					2	, Контрольная работа №3
20	3	Тема 3.3 Понятие односторонней функции. Шифрсистема RSA. Шифрсистема Эль-Гамаля	2		2		5	9	, тест
21	3	Тема 3.4 Криптографические протоколы. Криптографические хэш-функции	2		2			4	ПК2, по результатам контрольных работа 2, 3 и теста
22	3	Экзамен						27	ЭК
23		Всего:	36		18/6	2	25	108/6	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	3	РАЗДЕЛ 1 Теория алгоритмов. Тема: Машина Тьюринга	Машина Тьюринга	2 / 2
2	3	РАЗДЕЛ 1 Теория алгоритмов. Тема: Понятие сложности алгоритма и сложности задачи. Полиномиальные алгоритмы.	Понятие сложности алгоритма и сложности задачи. Полиномиальные алгоритмы.	2 / 2
3	3	РАЗДЕЛ 1 Теория алгоритмов. Тема: Примеры "быстрых" алгоритмов	Примеры "быстрых" алгоритмов	2
4	3	РАЗДЕЛ 1 Теория алгоритмов. Тема: Примеры NP-полных задач	Примеры NP-полных задач	2 / 2
5	3	РАЗДЕЛ 2 Теория кодирования. Тема: Алфавитное кодирование. Однозначное кодирование	Алфавитное кодирование. Однозначное кодирование	2
6	3	РАЗДЕЛ 2 Теория кодирования. Тема: Коды с минимальной избыточностью	Коды с минимальной избыточностью.	1
7	3	РАЗДЕЛ 2 Теория кодирования. Тема: Коды с обнаружением и исправлением ошибок	Коды с обнаружением и исправлением ошибок	1
8	3	РАЗДЕЛ 3 Криптография. Тема: Основные задачи криптографии. Исторический очерк и примеры шифров.	Основные задачи криптографии. Исторический очерк и примеры шифров.	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
9	3	РАЗДЕЛ 3 Криптография. Тема: Понятие односторонней функции. Шифрсистема RSA. Шифрсистема Эль-Гамаля	Понятие односторонней функции. Шифрсистема RSA. Шифрсистема Эль-Гамаля	2
10	3	РАЗДЕЛ 3 Криптография. Тема: Криптографические протоколы. Криптографические хэш-функции	Криптографические протоколы. Криптографические хэш-функции	2
			ВСЕГО:	18/6

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

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 организованна 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. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	3	РАЗДЕЛ 1 Теория алгоритмов. Тема 11: Примеры NP-полных задач	проработка учебного материала (по конспектам лекций учебной и научной литературе) (осн. [2, 4])	3
2	3	РАЗДЕЛ 1 Теория алгоритмов. Тема 3: Машина Тьюринга	проработка учебного материала (по конспектам лекций учебной и научной литературе) (осн. [2, 4])	5
3	3	РАЗДЕЛ 1 Теория алгоритмов. Тема 4: Тезис Тьюринга	проработка учебного материала (по конспектам лекций учебной и научной литературе) (осн. [2, 4])	2
4	3	РАЗДЕЛ 1 Теория алгоритмов. Тема 5: Кодирование МТ. Проблема самоприменимости. Алгоритмически неразрешимые задачи	проработка учебного материала (по конспектам лекций учебной и научной литературе) (осн. [2, 4])	3
5	3	РАЗДЕЛ 1 Теория алгоритмов. Тема 8: Примеры "быстрых" алгоритмов	проработка учебного материала (по конспектам лекций учебной и научной литературе) (осн. [2, 4])	4
6	3	РАЗДЕЛ 2 Теория кодирования. Тема 3: Коды с обнаружением и исправлением ошибок	проработка учебного материала; решение задач, упражнений (осн. [1, 6])	3
7	3	РАЗДЕЛ 3 Криптография. Тема 3: Понятие односторонней функции. Шифрсистема RSA. Шифрсистема Эль-Гамаля	проработка учебного материала; решение задач, упражнений (осн. [1, 3, 5])	5
			ВСЕГО:	25

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Основы классической криптологии: секреты шифров и кодов	Адаменко М.В.	М.: ДМК Пресс , 2012 http://e.lanbook.com/book/9123	Раздел 2 (1-128), Раздел 3 (129-254)
2	Математическая логика. Дискретные функции. Теория алгоритмов	Глухов М.М., Шишков А.Б.	М.: Лань, 2012 http://e.lanbook.com/view/book/4041/	Раздел 1 (283-341)
3	Информационная безопасность и защита информации	В.П. Мельников, С.А Клейменов, А.М. Петраков	М. : Издательский центр "Академия", 2009 НТБ МИИТа	Раздел 3 (5-325)
4	Дискретная математика	Плотников А.Д.	Минск: Новое знание , 2008 НТБ МИИТа	Раздел 1 (199-224)
5	Теория кодирования	Сидельников В.М.	Физматлит, 2008 http://e.lanbook.com/book/2311	Раздел 3 (4-320)
6	Кодирование и декодирование дискретного сообщения избыточными кодами	Шелухин В.И., Акинин М.Ю.	М.: МИИТ, 2008 НТБ МИИТа	Раздел 2 (3—67)

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
7	Основы криптографии	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	М.: Гелиос АРВ, 2002 НТБ МИИТа	Раздел 3 (7-468)
8	Защита компьютерной информации	Анин Б.Ю.	СПб.: БВХ-Петербург, 2000 НТБ МИИТа	Раздел 3 (5-382)
9	Сборник задач по дискретной математике	Гаврилов Г.П., Сапоженко А.А.	М.: Наука, 1977 НТБ МИИТа	Раздел 2 (230-252)
10	Основы теории информации	Кочнев В.Ф., Савина С.Н., Титов Е.В.	М.: МИИТ, 2002 НТБ МИИТа	Раздел 3 (3-46)
11	Введение в криптографию	Ященко В.В., Варновский Н.П., Нестеренко Ю.В. и др.	М.: МЦНМО, 2001 НТБ МИИТа	Раздел 3 (7-234)

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Можно скачать необходимую литературу:
http://www.miit.ru/
Информационные ресурсы/Библиотека
http://www.library.miit.ru

Учебно-методические издания в электронном виде
Вся предложенная в п. 7.1 и 7.2 литература имеется в электронном виде на кафедре и в начале семестра высылается студентам на электронный адрес группы.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

При организации обучения по дисциплине с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».
В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.
В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения аудиторных занятий и самостоятельной работы требуется стандартная учебная аудитория с доской, маркерами (мелом) и тряпкой, столами и стульями для студентов и преподавателя, стандартное освещение.
В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.
Допускается замена оборудования его виртуальными аналогами.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. В течение недели выбрать время (1 час) для работы с литературой в библиотеке.
3. При подготовке к практическим занятиям следующего дня необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи.

Рекомендации по использованию материалов учебно-методического комплекса.

Рекомендуется использовать методические указания по курсу, текст лекций преподавателя (если он имеется).

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта изучаются и книги. Легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему.

Дополнительно к изучению конспектов лекции необходимо пользоваться учебником. Рекомендуется после изучения очередного параграфа выполнить несколько упражнений на данную тему.

При подготовке к экзамену нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала – и самостоятельно решить по нескольку типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.

Для подготовки к занятиям и выполнения индивидуальной контрольной работы студентам предоставляются необходимая литература, методические пособия и рекомендации по выполнению в электронном виде. По необходимости проводятся консультации для успешного выполнения индивидуальных работ.
В качестве тренингов могут использоваться компьютерные тесты. Тестирование проводится в ауд. 1418. Электронная версия тестов имеется на кафедре.