

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

СОГЛАСОВАНО:

Выпускающая кафедра ВССиИБ
Заведующий кафедрой ВССиИБ



Б.В. Желенков

30 апреля 2020 г.

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Числовые методы криптографии

Направление подготовки:	<u>10.03.01 – Информационная безопасность</u>
Профиль:	<u>Безопасность компьютерных систем</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2020</u>

Одобрено на заседании Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии  Н.А. Клычева	Одобрено на заседании кафедры Протокол № 1 27 апреля 2020 г. Доцент  В.Е. Нутович
---	---

Рабочая программа учебной 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: 5665
Подписал: Доцент Нутович Вероника Евгеньевна
Дата: 27.04.2020

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цели освоения учебной дисциплины " Числовые методы криптографии":

Курс «Числовые методы криптографии» является математической дисциплиной, продолжающей теоретико-числовую и алгебраическую подготовку студентов. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются и в других дисциплинах, связанных с защитой информации. Цель преподавания дисциплины – обеспечить студентам знания в области теории чисел и алгебры, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.

Компетенции, приобретаемые студентами, применяются для научно-исследовательской деятельности.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: задачи теории чисел, алгебры и теории групп, работа в мультипликативной группе колец вычетов, применение свойств символов Лежандра и Якоби, тестов на простоту для натуральных чисел; использование методов разложения чисел и многочленов на множители.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Числовые методы криптографии" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Математическая логика и теория алгоритмов:

Знания: понятия, определения, термины; алгоритмы, способы решения задач курса принципы, основы, теории, законы; методы, алгоритмы, способы решения задач курса; основы, теории, законы, правила, используемые в курсе для изучения объектов курса

Умения: выделять объекты курса из окружающей среды; формулировать, выдвигать гипотезы о причинах возникновения той или иной ситуации; вычислять, оценивать величины; изменять, дополнять, адаптировать, развивать методы, алгоритмы, приемы, методики для решения конкретных задач; выбирать методы, алгоритмы, меры, средства, модели, законы, критерии для решения задач курса; оформлять данные, результаты работы на языке символов (терминов, формул), введенных и используемых в курсе; формулировать, выдвигать гипотезы о причинах возникновения той или иной ситуации (состояния, события), о путях (тенденциях) ее развития и последствиях; изменять, дополнять, адаптировать, развивать методы, алгоритмы, методики для решения конкретных задач;

Навыки: навыками систематизировать, дифференцировать факты, методы, задачи и т.д., самостоятельно формулируя основания для классификации; навыками ставить познавательные задачи и выдвигать гипотезы

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Преддипломная практика

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	ОПК-2 Способен использовать совокупность необходимых математических методов для решения задач обеспечения защиты информации.	ОПК-2.1 Знать необходимые математические методы для решения задач обеспечения защиты информации. ОПК-2.2 Уметь совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-2.3 Владеть навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.

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

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 ак. ч.).

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

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 5
Контактная работа	72	72,15
Аудиторные занятия (всего):	72	72
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	36	36
Самостоятельная работа (всего)	72	72
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

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 промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	5	Раздел 1 Алгебраические основы криптографии	14		12		24	50	
2	5	Тема 1.1 Идеалы в кольцах. Прямое произведение колец	4					4	ПК1
3	5	Тема 1.1 группы подстановок	2					2	
4	5	Тема 1.2 Факторкольца. Теоремы о гомоморфизмах колец	2					2	
5	5	Тема 1.2 цикловая запись подстановки. Ее порядок.	2					2	
6	5	Тема 1.3 подгруппы. теорема Лагранжа.	2					2	
7	5	Тема 1.5 группы	2					2	
8	5	Раздел 2 Теоретико-групповые основы криптографии	10		12		24	46	
9	5	Тема 2.4 циклические группы						0	ПК2
10	5	Тема 2.5 Сопряженные элементы и нормальные подгруппы	2					2	
11	5	Тема 2.6 Факторгруппы. Теоремы о гомоморфизмах групп	2					2	
12	5	Тема 2.7 Мультипликативная группа поля вычетов. Малая теорема Ферма	2					2	
13	5	Тема 2.8 Мультипликативная группа кольца вычетов. Теорема Эйлера. Функция	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Эйлера							
14	5	Тема 2.9 Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю	2					2	
15	5	Раздел 3 Квадратичные сравнения	4		4		8	16	
16	5	Тема 3.5 Квадраты в конечных полях	2					2	
17	5	Тема 3.6 Символ Лежандра и его вычисления	2					2	
18	5	Раздел 4 Нестандартные числовые системы	8		8		16	32	
19	5	Тема 4.7 p-адическая топология в \mathbb{Z}	2					2	
20	5	Тема 4.8 Кольцо целых p-адических чисел \mathbb{Z}_p	2					2	
21	5	Тема 4.9 Поле p-адических чисел \mathbb{Q}_p	2					2	
22	5	Тема 4.10 Геометрические модели \mathbb{Z}_p и \mathbb{Q}_p .	2					2	
23	5	Раздел 5 Итоговая аттестация						0	ЗаО
24		Тема 2.4 циклические группы							
25		Раздел 4.5 Геометрические модели \mathbb{Z}_p и \mathbb{Q}_p							
26		Всего:	36		36		72	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 36 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	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Группы. Группы подстановок.	4
2	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Идеалы в кольцах. Прямое произведение колец. Факторкольца.	4
3	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Цикловая запись подстановки. Ее порядок. Подгруппы. Теорема Лагранжа (интерактив)	4
4	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю (интерактив).	4
5	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Циклические группы. Сопряженные элементы и нормальные подгруппы.	4
6	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Мультипликативная группа поля и кольца вычетов. Малая теорема Ферма. Теорема Эйлера.	4
7	5	РАЗДЕЛ 3 Квадратичные сравнения	Символ Лежандра и его вычисление (интерактив)	4
8	5	РАЗДЕЛ 4 Нестандартные числовые системы	Кольцо целых p -адических чисел Z_p	4
9	5	РАЗДЕЛ 4 Нестандартные числовые системы	Поле p -адических чисел Q_p . Геометрические модели Z_p и Q_p	4
ВСЕГО:				36/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Числовые методы криптографии» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100% являются традиционными классически-лекционными (объяснительно-иллюстративные).

Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объеме 12 часов. Остальная часть практического курса (6 часов) проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения.

Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к текущему и промежуточному контролю, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных заданий с использованием компьютеров или на бумажных носителях.

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	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Идеалы в кольцах. Прямое произведение колец	4
2	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Факторкольца. Теоремы о гомоморфизмах колец	4
3	5	РАЗДЕЛ 1 Алгебраические основы криптографии	группы	4
4	5	РАЗДЕЛ 1 Алгебраические основы криптографии	группа подстановок	4
5	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Цикловая запись подстановки. Ее порядок.	4
6	5	РАЗДЕЛ 1 Алгебраические основы криптографии	Подгруппы. Теорема Лагранжа.	4
7	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Циклические группы	4
8	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Сопряженные элементы и нормальные подгруппы	4
9	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Факторгруппы. Теоремы о гомоморфизмах групп	4
10	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Мультипликативная группа поля вычетов. Малая теорема Ферма.	4
11	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Мультипликативная группа кольца вычетов. Теорема Эйлера. Функция Эйлера	4
12	5	РАЗДЕЛ 2 Теоретико-групповые основы криптографии	Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю	4
13	5	РАЗДЕЛ 3 Квадратичные сравнения	Квадраты в конечных полях	4
14	5	РАЗДЕЛ 3 Квадратичные сравнения	Символ Лежандра и его вычисления	4
15	5	РАЗДЕЛ 4 Нестандартные числовые системы	Геометрические модели Z_p и Q_p	4
16	5	РАЗДЕЛ 4 Нестандартные числовые системы	Поле p -адических чисел Q_p	4
17	5	РАЗДЕЛ 4 Нестандартные числовые системы	p -адическая топология в Z	4

18	5	РАЗДЕЛ 4 Нестандартные числовые системы	Кольцо целых p-адических чисел Z_p	4
ВСЕГО:				72

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 современной криптографии	С.Г. Баричев, В.В. Гончаров, Р.Е. Серов	Горячая линия - Телеком, 2011 НТБ МИИТ	Все разделы
2	Введение в криптографию	В.В. Яценко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Яценко	МЦНМО: "ЧеРо", 2012 НТБ МИИТ	Все разделы
3	Введение в теоретико-числовые методы криптографии	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	СПб: «Лань», 2010 НТБ МИИТ	Все разделы
4	Введение в криптосистемы с открытым ключом	Молдовян Н. А., Молдовян А.А	СПб.: БХВ-Петербург, 2005 НТБ МИИТ	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
-------	--------------	-----------	--------------------------------------	--

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

<http://library.miit.ru/> - электронно-информационная система НТБ МИИТ

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

Не требуется

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

Требования к аудиториям (помещениям, кабинетам) для проведения занятий с указанием соответствующего оснащения

- Доска, мел, тряпка (губка) для стирания; компьютерное и мультимедийное оборудование: компьютер, проектор, экран;

Требования к программному обеспечению при прохождении учебной дисциплины

- пакет прикладных обучающих программ: MATHCAD, Maple

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

Регулярно выполнять домашние задания, изучать дополнительные материалы, повторять темы из предыдущих семестров. Интересующимся студентам рекомендуется участвовать

в студенческих олимпиадах.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления. Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке специалиста важны не только серьезная теоретическая подготовка. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает

повышение качества образовательного процесса и входит как приложение в состав рабочей программы дисциплины.