

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 - программы бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Числовые методы криптографии

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность 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: 5665
Подписал: заведующий кафедрой Нутович Вероника
Евгеньевна
Дата: 16.01.2023

1. Общие сведения о дисциплине (модуле).

Цели освоения учебной дисциплины Б1.В.ОД.9 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. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности .

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

Знать:

понятия, определения, термины; алгоритмы, способы решения задач курса принципы, основы, теории, законы; методы, алгоритмы, способы решения задач курса

Знать:

основы, теории, законы, правила, используемые в курсе для изучения

объектов курса

Уметь:

выделять объекты курса из окружающей среды; формулировать, выдвигать гипотезы о причинах возникновения той или иной ситуации; вычислять, оценивать величины

Уметь:

изменять, дополнять, адаптировать, развивать методы, алгоритмы, приемы, методики для решения конкретных задач

Уметь:

выбирать методы, алгоритмы, меры, средства, модели, законы, критерии для решения задач курса

Уметь:

оформлять данные, результаты работы на языке символов (терминов, формул), введенных и используемых в курсе

Уметь:

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

Владеть:

навыками систематизировать, дифференцировать факты, методы, задачи и т.д., самостоятельно формулируя основания для классификации

Владеть:

навыками ставить познавательные задачи и выдвигать гипотезы

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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	Сем. №5
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 96 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	Алгебраические основы крипто-фии Тема 1.1 Идеалы в кольцах. Прямое произведение колец Тема 1.2 группы подстановок Тема 1.3 Факторкольца. Теоремы о гомоморфизмах колец Тема 1.4 цикловая $\mathbb{Z}$ -апись подстановки. Ее порядок. Тема 1.5 подгруппы. теорема Лагранжа. Тема 1.6 группы
2	Теоретико-групповые основы крипто-фии Тема 2.1 циклические группы Тема 2.2 Сопряженные элементы и нормальные подгруппы

№ п/п	Тематика лекционных занятий / краткое содержание
	Тема 2.3 Факторгруппы. Теоремы о гомоморфизмах групп Тема 2.4 Мультипликативная группа поля вычетов. Малая теорема Ферма Тема 2.5 Мультипликативная группа кольца вычетов. Теорема Эйлера. Функция Эйлера Тема 2.6 Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю
3	Квадратичные сравнения Тема 3.1 Квадраты в конечных полях Тема 3.2 Символ Лежандра и его вычисление
4	Нестандартные числовые системы Тема 4.1 p -адическая топология в $\mathbb{Z}$ Тема 4.2 Кольцо целых p -адических чисел $\mathbb{Z}_p$ Тема 4.3 Поле p -адических чисел $\mathbb{Q}_p$ Тема 4.4 Геометрические модели $\mathbb{Z}_p$ и $\mathbb{Q}_p$. Тема 4.5 циклические группы Тема 4.6 Геометрические модели $\mathbb{Z}_p$ и $\mathbb{Q}_p$

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Группы. Группы подстановок.
2	Идеалы в кольцах. Прямое произведение колец. Факторкольца.
3	Цикловая запись подстановки. Ее порядок. Подгруппы. Теорема Лагранжа (интерактив)
4	Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю (интерактив).
5	Циклические группы. Сопряженные элементы и нормальные подгруппы.
6	Мультипликативная группа поля и кольца вычетов. Малая теорема Ферма. Теорема Эйлера.
7	Символ Лежандра и его вычисление (интерактив)
8	Кольцо целых p -адических чисел $\mathbb{Z}_p$
9	Поле p -адических чисел $\mathbb{Q}_p$. Геометрические модели $\mathbb{Z}_p$ и $\mathbb{Q}_p$

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Идеалы в кольцах. Прямое произведение колец
2	Факторкольца. Теоремы о гомоморфизмах колец
3	группы
4	группа подстановок
5	Цикловая запись подстановки. Ее порядок.
6	Подгруппы. Теорема Лагранжа.
7	Циклические группы
8	Сопряженные элементы и нормальные подгруппы
9	Факторгруппы. Теоремы о гомоморфизмах групп
10	Мультипликативная группа поля вычетов. Малая теорема Ферма.
11	Мультипликативная группа кольца вычетов. Теорема Эйлера. Функция Эйлера
12	Порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю
13	Квадраты в конечных полях
14	Символ Лежандра и его вычисления
15	Геометрические модели Z_p и Q_p
16	Поле p -адических чисел Q_p
17	p -адическая топология в Z
18	Кольцо целых p -адических чисел Z_p
19	Подготовка к промежуточной аттестации.
20	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Основы современной криптографии С.Г. Баричев, В.В. Гончаров, Р.Е. Серов Однотомное издание Горячая линия - Телеком , 2002	НТБ (фб.); НТБ (чз.1); НТБ (чз.2)
2	Введение в криптографию В.В. Яценко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Яценко Однотомное издание МЦНМО: "ЧеРо" , 2000	НТБ (фб.); НТБ (чз.2)
3	Введение в теоретико-числовые методы криптографии М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин Однотомное издание Лань , 2010	НТБ
4	Введение в криптосистемы с открытым ключом Н. А.	НТБ

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

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

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

пакет прикладных обучающих программ: MATHCAD, Maple

8. 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;

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

10. Оценочные материалы.

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

Авторы:

старший преподаватель кафедры
«Цифровые технологии управления
транспортными процессами»

В.П. Посвянский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Заведующий кафедрой ЦТУТП

В.Е. Нутович

Председатель учебно-методической
комиссии

Н.А. Клычева