

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: 01.09.2022

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- обеспечение подготовки в одной из важных областей, находящихся на границе теории чисел, информатики и криптографии;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография.

Задачами дисциплины являются:

- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография;
- ознакомление с основами классической и современной теории чисел, имеющими практические приложения к решению некоторых важных криптографических задач.

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;
- 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;
- изменять, дополнять, адаптировать, развивать методы, алгоритмы, приемы, методики для решения конкретных задач;
- оформлять данные, результаты работы на языке символов (терминов, формул), введенных и используемых в курсе.

Владеть:

- навыками систематизировать, дифференцировать факты, методы, задачи и т.д., самостоятельно формулируя основания для классификации;
- 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 | Семестр №5 |
| Контактная работа при проведении учебных занятий (всего): | 66 | 66 |
| В том числе: | | |
| Занятия лекционного типа | 34 | 34 |
| Занятия семинарского типа | 32 | 32 |

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 78 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 крипт-фии Рассматриваемые вопросы: - идеалы в кольцах. Прямое произведение колец; - группы подстановок. |
| 2 | Алгебраические основы криптографии Рассматриваемые вопросы: - факторкольца. Теоремы о гомоморфизмах колец; - цикловая запись подстановки. Ее порядок; - подгруппы. Теорема Лагранжа. |
| 3 | Теоретико-групповые основы крипт-фии Рассматриваемые вопросы: - циклические группы; - сопряженные элементы и нормальные подгруппы; - факторгруппы. Теоремы о гомоморфизмах групп. |
| 4 | Теоретико-групповые основы криптографии Рассматриваемые вопросы: - мультипликативная группа поля вычетов. Малая теорема Ферма; - мультипликативная группа кольца вычетов. Теорема Эйлера. Функция Эйлера; - порядок элемента в кольце вычетов. Алгоритм быстрого возведения в степень по модулю. |
| 5 | Нестандартные числовые системы Рассматриваемые вопросы: - p -адическая топология в \mathbb{Z} ; - кольцо целых p -адических чисел \mathbb{Z}_p . |
| 6 | Нестандартные числовые системы Рассматриваемые вопросы: - циклические группы; - геометрические модели \mathbb{Z}_p и \mathbb{Q}_p . |
| 7 | Нестандартные числовые системы Рассматриваемые вопросы: - поле p -адических чисел \mathbb{Q}_p ; - геометрические модели \mathbb{Z}_p и \mathbb{Q}_p . |
| 8 | Квадратичные сравнения Рассматриваемые вопросы: - квадраты в конечных полях; - символ Лежандра и его вычисление. |

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. |

| № п/п | Тематика практических занятий/краткое содержание |
|-------|---|
| 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 вычисления (интерактив) |
| 8 | Кольцо целых p -адических чисел Z_p |
| 9 | Поле p -адических чисел Q_p . Геометрические модели Z_p и Q_p |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|-------|--|
| 1 | Изучение дополнительной литературы |
| 2 | Подготовка к практическим занятиям |
| 3 | Подготовка к промежуточной аттестации. |
| 4 | Подготовка к текущему контролю. |

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

| № п/п | Библиографическое описание | Место доступа |
|-------|---|-----------------------------------|
| 1 | С.Г. Баричев, В.В. Гончаров, Р.Е. Серов Основы современной криптографии, Горячая линия - Телеком, 2002. - 175 с.; - ISBN 5-93517-075-2 Однотомное издание | 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. - 3. изд., испр. - Москва : МЦНМО : ЧеРо, 2000. - 287 с. - ISBN 5-900916-65-0 Однотомное издание | НТБ (фб.); НТБ (чз.2) |
| 3 | . В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0 Однотомное издание | НТБ РУТ (МИИТ) |
| 4 | Введение в криптосистемы с открытым ключом: проблематика криптографии, элементы теории чисел, двухключевые криптосистемы, системы электрон. цифровой подписи с составным модулем, открытое распределение ключей и открытое шифрование, упр. ключами и протоколы / Н. А. Молдовян, А. А. Молдовян. - СПб. : БХВ-Петербург, 2005 (ППП Тип. Наука). - 286 с. : | НТБ РУТ (МИИТ) |

| | |
|---|--|
| ил.; 24 см. - (Учебное пособие).; ISBN 5-94157-563-7 (в пер.) | |
|---|--|

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

Официальный сайт РУТ (МИИТ) (<https://www.miit.ru/>).

Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>).

Образовательная платформа «Юрайт» (<https://urait.ru/>).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>).

Электронно-библиотечная система ibooks.ru (<http://ibooks.ru/>).

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

пакет прикладных обучающих программ: МATHCAD, Maple

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

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 ЦТУТП

В.Е. Нутович

Председатель учебно-методической
комиссии

Н.А.Клычева