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
01.03.02 Прикладная математика и информатика,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Компьютерная безопасность

Направление подготовки: 01.03.02 Прикладная математика и информатика

Направленность (профиль): Математические модели в экономике и технике

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: 10.06.2021

1. Общие сведения о дисциплине (модуле).

В курсе «Компьютерная безопасность» изучаются основные математические методы криптографии. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической криптографии и ее прикладных методов, 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: алгебраические и теоретико-числовые основы криптографии, криптосистемы RSA, Эль-Гамаля, Рабина, а также криптопротоколы Диффи-Хеллмана, Шнорра, Блюма и некоторые другие. использование частотных характеристик открытых текстов для анализа простейших шифров замены и перестановки, применение стандартов в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных систем, изучение современной литературе по криптографии. В результате освоения дисциплины студент будет владеть криптографическими понятиями, стандартными криптографическими алгоритмами и протоколами, реализуемыми на компьютерах, приёмами математического моделирования в шифровании. владеть знаниями и опытом, связанным с теорией алгебраических чисел (символ Лежандра, символ Якоби, квадратичный закон взаимности Гаусса).

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-4 - Уметь ставить цели создания системы, разрабатывать концепцию системы и требования к ней, выполнять декомпозицию требований к системе.

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

Знать:

алгебраические и теоретико-числовые основы криптографии, криптосистемы RSA, Эль-Гамаля, а также криптопротоколы Диффи-Хеллмана, Блюма и некоторые другие.

Уметь:

использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки, применять стандарты в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных систем, разбираться в современной литературе по криптографии.

Владеть:

криптографическими понятиями, стандартными криптографическими алгоритмами и протоколами, реализуемыми на компьютерах, приёмами математического моделирования в шифровании, владеть знаниями и опытом, связанным с теорией алгебраических чисел (символ Лежандра, символ Якоби, закон взаимности Гаусса).

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 1
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 80 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 и теоретико-числовые основы криптографии Рассматриваемые вопросы: - тест Миллера-Рабина; - построение больших простых чисел по алгоритму Маурера.
2	Алгебраические и теоретико-числовые основы криптографии Рассматриваемые вопросы: - символ Лежандра; - базовые алгоритмы.
3	Алгебраические и теоретико-числовые основы криптографии Рассматриваемые вопросы: - кольца вычетов; - прямое произведение колец; - конечные поля.
4	Криптосистемы Рассматриваемые вопросы: - шифры замены и шифры перестановки; - результаты К. Шеннона об абсолютно (максимально) стойких шифрах.
5	Криптосистемы Рассматриваемые вопросы: - перестановочные шифры: генерирование случайных перестановок; - система шифрования RSA. Система шифрования Эль-Гамаля.
6	Криптосистемы Рассматриваемые вопросы: - цели и задачи криптографии; - история криптографии; - основные понятия.
7	Криптопротоколы Рассматриваемые вопросы: - понятие криптопротокола; - виды криптоколов.
8	Криптопротоколы Рассматриваемые вопросы: - протокол Диффи-Хеллмана; - протокол Блюма.
9	Криптопротоколы Рассматриваемые вопросы: - протоколы электронной подписи; - протоколы разделения секрета.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Алгебраические и теоретико-числовые основы криптографии В результате работы на практических занятиях студент учится на конкретных примерах искать кольца вычетов и их прямое произведение.
2	Алгебраические и теоретико-числовые основы криптографии В результате работы на практическом занятии студент получает навык искать символ Лежандра, применять базовые алгоритмы
3	Алгебраические и теоретико-числовые основы криптографии В результате работы на практическом занятии студент осваивает тест Миллера-Рабина, учится строить большие простые числа по алгоритму Маурера.
4	Криптосистемы В результате работы на практических занятиях студент учится на конкретных примерах строить шифры замены и шифры перестановки.
5	Криптосистемы В результате работы на практическом занятии студент изучает перестановочные шифры и учится генерировать случайные перестановки
6	Криптосистемы В результате работы на практическом занятии студент учится использовать систему шифрования RSA и Эль-Гамаля.
7	Криптопротоколы В результате работы на практических занятиях студент учится строить протоколы Диффи-Хеллмана.
8	Криптопротоколы В результате работы на практических занятиях студент учится строить протоколы Блюма.
9	Криптопротоколы В результате работы на практических занятиях студент учится строить протоколы электронной подписи и разделения секрета.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение 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	Мартынов Л.М. Алгебра и теория чисел для криптографии. стер. — Санкт-Петербург : Лань, 2022. - 456 с. - ISBN 978-5-8114-9346-3	https://e.lanbook.com/book/189446

2	Коржик В.И. Основы криптографии. Санкт-Петербург : Интермедия, 2017. - 312 с. - ISBN 978-5-89160-097-3	https://e.lanbook.com/book/161359
3	Глухов М.М. Введение в теоретико-числовые методы криптографии. Санкт-Петербург : Лань, 2022. - 400 с. - ISBN 978-5-8114-1116-0	https://e.lanbook.com/book/210746
4	Пономарчук Ю.В. Основы анализа шифров классической криптографии. Хабаровск : ДВГУПС, 2019. - 113 с. - ISBN нет	https://e.lanbook.com/book/179357

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

единая коллекция цифровых образовательных ресурсов (http://window.edu.ru);

научно-техническая библиотека РУТ (МИИТ) (http://library.miit.ru/).

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

Программное обеспечение не требуется.

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:

Ю.С. Семенов

Согласовано:

Заведующий кафедрой ЦТУТП	В.Е. Нутович
Председатель учебно-методической комиссии	Н.А.Клычева