

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 27.09.2023 08:20:54
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семькина

Семькина
« 4 » 09 2023 г.
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
университет

Рабочая программа дисциплины (с аннотацией)

Методы и средства криптографической защиты информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:

Никонов В. В. *Никонов*

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области использования и проектирования и средств криптографической защиты информации, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

- получение базовых знаний и умений, связанных с основными понятиями средств криптографической защиты информации;
- получение теоретических знаний о роли и назначении различных криптографических систем;
- обучения студентов общим принципам и методам построения криптографических систем;

получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью средств криптографической защиты информации.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Языки программирования», «Алгебра», «Теоретико-числовые методы в криптографии».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Методы алгебраической геометрии в криптографии», «Криптографические протоколы», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 7 зачетные единицы, 252 академических часов, в том числе:

контактная аудиторная работа: лекции – 64 ч., в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 47 ч., практические занятия – 17 ч., в т.ч. практическая подготовка – 8 ч.;

самостоятельная работа: 124 ч., в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1 Применяет основы теории чисел в криптографии и других дисциплинах

<p>ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p>	<p>ОПК-9.1 Использует криптографические алгоритмы на практике при решении задач криптографическими методами</p>
<p>ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>ОПК-10.1 Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел</p>
	<p>ОПК-10.2 Разворачивает инфраструктуру открытых ключей для решения криптографических задач</p>
	<p>ОПК-10.4 Применяет различные подходы к разработке и анализу безопасности криптографических протоколов</p>

5. Форма промежуточной аттестации и семестр прохождения – зачет в 7 семестре, экзамен в 8 семестре.

6. Язык преподавания русский.