

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 17.10.2023 14:21:12
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)

Криптографические протоколы

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Семькина Н. А. *Семькина*

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 проектирования и построения криптографических протоколов, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

- 1) получение базовых знаний и умений, связанных с основными понятиями криптографических протоколов;
- 2) формирование навыков решения прикладных задач, решаемых с помощью криптопротоколов и умения применять различные методы и алгоритмы построения криптографических протоколов.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации», «Теоретико-числовые методы в криптографии».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 ч., в т.ч. практическая подготовка – 0 часов;

практические занятия – 34 ч., в т.ч. практическая подготовка – 7 ч.;

самостоятельная работа: 40 ч.

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-9. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-9.2 Проводит анализ криптографических протоколов, в том числе с использованием автоматизированных средств
ОПК-10. Способен анализировать тенденции развития методов и средств	ОПК-10. Разворачивает инфраструктуру открытых ключей для решения криптографических задач

<p>криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</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 9 семестре.

6. Язык преподавания русский.