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

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Методы алгебраической геометрии в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Семыкина Н. А.

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 на эллиптических кривых, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

1) получение базовых знаний и умений, связанных с основными понятиями алгебраической геометрии;

2) получение теоретических знаний о роли и назначении различных криптосистем на базе эллиптических кривых;

3) изучение общих принципов и методов построения криптографических систем на основе эллиптических кривых;

4) изучение различных схем электронной подписи и современных стандартов формирования проверки ЭЦП.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Методы и средства криптографической защиты информации», «Алгебра».

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 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 17 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 часа.

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-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	**ОПК-3.1** Производит стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ
ОПК-8. Способен применять методы научных исследований при проведении разработок в	**ОПК-8.1** Применяет основы теории чисел в криптографии и других дисциплинах

области обеспечения безопасности компьютерных систем и сетей	
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	**ОПК-9.1.** Использует криптографические алгоритмы на практике при решении задач криптографическими методами
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**ОПК-10.1.** Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**ОПК-2.1.1.** Использует в профессиональной деятельности криптографические алгоритмы и реализует их программно
	ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации
ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации	**ОПК-2.2.1.** Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы
	ОПК-2.2.2. Разрабатывает математические модели, реализуемые в средствах защиты информации

5. Форма промежуточной аттестации и семестр прохождения – зачет в 9 семестре.

6. Язык преподавания русский**.**