Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теоретико-числовые методы в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 4 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составители:

ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

1. Наименование дисциплины (модуля) в соответствии с учебным планом

Теоретико-числовые методы в криптографии.

2. Цель и задачи дисциплины (модуля)

Целью освоения дисциплины (модуля) является:

формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических систем, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными теоретико-числовыми методами в криптографии;
- получение теоретических знаний о роли и назначении различных алгоритмов;
- получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью теоретико-числовых методов;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла. Для освоения дисциплины студент должен владеть основными понятиями криптографии, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам, языки программирования, криптографические методы защиты информации, алгебра, математическая логика и теория алгоритмов. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

___2___ зачетных единиц, __72__ академических часов, **в том числе контактная работа:** лекции _18__ часов, практические занятия _18____ часов, , **самостоятельная работа:** ___36__ часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (модулю)**
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** криптографической терминологией. **Уметь:** уметь учитывать современные достижения информационных технологий в своей профессиональной деятельности. **Знать:** о видах информации, подлежащей шифрованию.
Базовый **ПСК-2.1.** способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	**Владеть:** навыками применения теории чисел в криптографии; навыками применения основных вычислительных алгоритмов в кольцах вычетов и кольцах многочленов. **Уметь:** применять теоретико-числовые методы и алгоритмы для защиты информации; исследовать и решать системы сравнений по произвольному модулю; представлять действительные числа цепными дробями; строить большие простые числа, применять алгоритмы проверки чисел на простоту; построения больших простых чисел; применять алгоритмы разложения чисел и многочленов на множители. **Знать:** теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации.

6. Форма промежуточной аттестации: зачет.

7. Язык преподавания русский**.**